FORM PTO-1390 (REV. 11-2000) U S DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY 'S DOCKET NUMBER: 110273.500US1

US APPLICATION NO (If known, see 37 CFR 1 5): 10/018095

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/US00/16381	15 June 2000	15 June 1999

TITLE OF INVENTION
SECURE, ACCOUNTABLE, MODULAR AND PROGRAMMABLE SOFTWARE TRAC

APPLICANT(S) FOR DO/EO/US
Richard C. WALKER

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☑ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☐ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.
4. ☑ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☑ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is attached hereto (required only if not communicated by the International Bureau).
   b. ☐ has been communicated by the International Bureau.
   c. ☑ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. ☐ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☑ Amendments to the claims of the International Aplication under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are attached hereto (required only if not communicated by the International Bureau).
   b. ☑ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☐ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ An English lanugage translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 20 below concern document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☑ A FIRST preliminary amendment.
14. ☐ A SECOND or SUBSEQUENT preliminary amendment.
15. ☐ A substitute specification.
16. ☐ A change of power of attorney and/or address letter.
17. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
18. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
19. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. ☐ Other items or information:

JC13 Rec'd PCT/PTO 14 DEC 2001

U.S. APPLICATION NO (if known, see 37 CFR 1.5) 10/018095	INTERNATIONAL APPLICATION NO PCT/US00/16381	ATTORNEY'S DOCKET NUMBER 110273.500US1

21. ☑ The following fees are submitted:				CALCULATIONS	PTO USE ONLY
BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)):					
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO **$1000.00**					
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO **$860.00**					
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$710.00**					
International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) **$690.00**					
International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) **$100.00**					
ENTER APPROPRIATE BASIC FEE AMOUNT =				$ 100.00	
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).				$	
CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	$	
Total claims	20 - 20 =	0	x **$18.00**	$ 0.00	
Independent claims	2 - 3 =	0	x **$80.00**	$ 0.00	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ **$270.00**	$ 0.00	
TOTAL OF ABOVE CALCULATIONS =				$ 100.00	
☑ Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2. +				$ 50.00	
SUBTOTAL =				$ 50.00	
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)).				$ 0.00	
TOTAL NATIONAL FEE =				$ 50.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +				$	
TOTAL FEES ENCLOSED =				$ 50.00	
				Amount to be refunded:	$
				charged:	$

a. ☐ A check in the amount of $ ______________ to cover the above fees is enclosed.

b. ☑ Please charge my Deposit Account No. 08-0219 in the amount of $ 50.00 to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☑ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 08-0219. A duplicate copy of this sheet is enclosed.

d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137 (a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO

Irah H. Donner
Hale and Dorr LLP
1455 Pennsylvania Avenue, NW
Washington, DC 20004-1008

SIGNATURE

Irah H. Donner

NAME

35,120

REGISTRATION NUMBER

Docket No.: 110273.500US1

PATENT/OFFICIAL

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of		
Richard C. Walker		
Serial No.	10/018,095	Group Art Unit:
Filed:	December 14, 2001	Examiner:

For: SECURE, ACCOUNTABLE, MODULAR AND PROGRAMMABLE SOFTWARE TRAC

PRELIMINARY AMENDMENT

Honorable Commissioner for Patents
Washington, D. C. 20231

Sir:

The following amendments and remarks are respectfully submitted.

IN THE SPECIFICATION

Please amend the specification as follows:

Please amend page 1 of the specification as indicated in the attached Appendix A (Marked-up Copy of Amended Specification). A clean copy of the amendments to the specification is attached as Appendix B (Replacement Page of Amended Specification).

IN THE CLAIMS

Please add claims 21-75 as indicated in the attached Appendix C. A complete set of claims is attached on Appendix D.

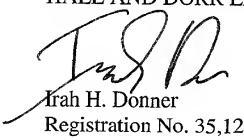
REMARKS

This Preliminary Amendment is submitted to improve the form of the specification and claims as originally filed. It is respectfully requested that this Preliminary Amendment be favorably examined and entered in the above-referenced application.

AUTHORIZATION

The Commissioner is hereby authorized to charge any additional fees which may be required for this Amendment, or credit any overpayment to deposit account no. 08-0219. In the event that an extension of time is required, or which may be required in addition to that requested in a petition for an extension of time, the Commissioner is requested to grant a petition for that extension of time which is required to make this response timely and is hereby authorized to charge any fee for such an extension of time or credit any overpayment for an extension of time to deposit account no. 08-0219.

Respectfully submitted,
HALE AND DORR LLP



Irah H. Donner
Registration No. 35,120

1455 Pennsylvania Avenue, N.W.
Washington, DC 20004-1008
(202) 942-8400
Date: 1/24/02
IHD/sed

Appendix A
(marked-up copy of amended specification)

Please amend page 1 of the specification as follows:

RELATED APPLICATIONS

This [patent] application is a National Phase application of International Application No. PCT/US00/16381, filed June 15, 2000, which in turn claims priority from U.S. Provisional Patent Application No. [60/---,---] 60/200,872, filed May 1, 2000 [(110273-700)] (110273-120); U.S. Provisional Application No. 60/176,818, filed January 19, 2000 (110273-401); and U.S. Provisional Application No. 60/139,759, filed June 15, 1999 (110273.500), all incorporated herein by reference.

Appendix B
(replacement page of amended specification)

RELATED APPLICATIONS

This application is a National Phase application of International Application No. PCT/US00/16381, filed June 15, 2000, which in turn claims priority from U.S. Provisional Patent Application No. 60/200,872, filed May 1, 2000 (110273-120); U.S. Provisional Application No. 60/176,818, filed January 19, 2000 (110273-401); and U.S. Provisional Application No. 60/139,759, filed June 15, 1999 (110273.500), all incorporated herein by reference.

Appendix C
(new claims to be added)

21. (NEW) A real-time vehicle or equipment management system according to claim 1, wherein an electronic serial number (ESN) allows each element within the matrix to be securely and accurately tracked, inventoried or controlled, either through a local control loop or remotely, by an authorized application or agency.

22. (NEW) A real-time vehicle or equipment management system according to claim 1, wherein an electronic serial number includes the basis for digital encryption of information passed between the PFN device and the controlling entity with local network processing nodes through public communications channels such as the phone lines or Internet initiated in many cases wirelessly from mobile PFNs accompanied by their Mobile Identification Number.

23. (NEW) A real-time vehicle or equipment management system according to claim 1, wherein this programmable software and/or any other accountable software program that performs automated and remote control and/or robotics functions as a result of programming that can authorize, authenticate and preserves commands and save feedback data as a TRAC software program and proprietary to this technology and its nature and scope.

24. (NEW) A real-time vehicle or equipment management system according to claim 1, wherein at least one non-volatile memory storage and controlled events are in secured environments so that it is highly tamper resistant through physical means and equally protected through electrical means and tamper resistant software programming to become an agreed upon standard for accountable reliable and trusted software commands and record keeping for passive and aggressive remote control and robotics to analyze, judge, evaluate, value, appraise and monitor, manage and control at least one of vehicle use, machine use, equipment use, facility or installation functions, perform financial transactions in real time and in stationary and mobile settings.

25. (NEW) A real-time vehicle or equipment management system according to claim 1, wherein accountable data is provided to an E-mail address web site and/or through the use of the World Wide Web and/or Internet Protocol (IP) for at least one of financial purposes, government uses, service providers, social purposes, environmental purposes.

26. (NEW) A real-time vehicle or equipment management system according to claim 1, wherein at least one of modular and programmable routines are determined by the existing hardware and operating system firmware or software for any application responsively connectable through any communication medium by querying each component device attached through a PFN/TRAC system and/or piece of equipment to determine if said connectable component is legitimate and cleared for safe public use.

27. (NEW) A real-time vehicle or equipment management system according to claim 1, wherein a registry includes all applicable government agencies with their own access to the Registry and/or network with encrypted codes and Identity command strings which are communicative

and also access for the general public and their Private Encrypted Identity codes (PINs, etc.) access to same said registry.

28. (NEW) A real-time vehicle or equipment management system according to claim 1, wherein a registry is accessible by a plurality of manufacturers on a worldwide scale with a plurality of security protocols in the marketing of component, devices and equipment and manufacture must provide a program to be given authorization for sale, and wherein the registry will not activate either the component device and/or piece of equipment without authorization, and resale of the component device or piece of equipment will be requested upon each connectable and queried to respond to the nature of the new install as the registry is contacted and requested to activate the unit.

29. (NEW) A real-time vehicle or equipment management system according to claim 1, wherein a registry including encryption on the Web will support any and all payment industry software.

31. (NEW) A real-time vehicle or equipment management system according to claim 1, wherein record keeping requires at least one of terminal and device electrical serial numbers and personal identification numbers as part of its authorization and authentication program with the time date and any geographic location coordinates or address of all the equipment and systems participating or performing entries or accessing any application folder or event file in storage at any location or part of the registry.

32. (NEW) A real-time vehicle or equipment management system according to claim 1, wherein a host piece of equipment will not operate any of its accessories unless it is provided the correct signal from the registry or a security network, and wherein commercial off the shelf (COTS) products utilize the security functions, resulting in immediate and cost effective conversions.

33.(NEW) A portable primary focal node (PFN) tracking device that is worn by an individual and reports a location to at least one web address through a public server gateway node, or publicly owned provider node using any type of communication system, an additional claim is made for the networking use of any multi-communication capable PFN to relay or repeat shorter range signals for personally worn PFN devices, wherein said PFN includes hardware and programmable and or modular software or firmware termed TRAC which functions as a Trusted Remote Activity Controller providing robotics or automated and remote control accountability by recording event data local and redundantly in remote memory storage, for communication components and computer hardware systems as determined by any industry or government standards efforts and protocols, for interfacing with activity controls, sensors, or discretes in any vehicle, machine, or as part of any equipment or on any person, animal, living entity or for any arbitrary use as a free standing piece of accountable telemetry or control equipment.

34. (NEW) A real-time or equipment management system according to claim 1 that serves as an accountable end user instruction center or audio tutor to deliver E-learning and educational programming via the PFN TRAC System and discretes.

35. (NEW) A real-time or equipment management system according to claim 1 that can be converted to the highest government and military security protocols, e.g., DES and DET, for national security public safety, nation briefing functions.

36. (NEW) A real-time or equipment management system according to claim 1 that provides write one-time memory storage locally as a secure accountable function to track and identify the source of any tampering or hacking to the PFN/TRAC System.

37. (NEW) A claim is made for a local Primary Focal Node termed a PFN to have hardware and programmable and or modular software or firmware termed TRAC which functions as a Trusted Remote Activity Controller providing robotics or automated and remote control accountability by recording event data local and redundantly in remote memory storage, for communication components and computer hardware systems as determined by any industry or government standards efforts and protocols, for interfacing with activity controls, sensors, or discretes in any vehicle, machine, or as part of any equipment or on any person, animal, living entity or for any arbitrary use as a free standing piece of accountable telemetry or control equipment.

38. (NEW) An additional claim is made for a connectable system software termed TRACS to be operational with the PFN/TRAC local devices and capable of receiving PFN routing of the numerous sub programs and the application specific data strings as detailed in all PFN application specifications and creating a secure redundant event memory storage.

39. (NEW) An additional claim to claim 37 is made for the entire system to provide accurate records of operation and failure as determined by a standards effort to be considered a Trusted system.

40. (NEW) A further claim is made according to claim 37 for any fail safe or backup system necessary to be qualified as a trusted device and system as determined by any standards effort at any time in the future.

41. (NEW) A claim is made according to claim 37 that this software and hardware be in a protective encasement application specific to it's environment and purpose and also to be determined by any standards effort at any time in the future.

42. (NEW) A claim is a made according to claim 37 that the software and hardware have no special encasement provision. and can be constructed in any functional configuration and format.

43. (NEW) A claim is made according to claim 37 for an electric certified seal mechanism to secure any encased area and to determine if the area has been breached; this device and system is also to be determined by any stands effort or law.

44. (NEW) A claim is made according to claim 37 for a mechanical locking device or system to secure any encased area.

45. (NEW) A claim is made according to claim 37 to refer to this modular and programmable software program or any other programming that performs automated accountable remote control and or robotics functions that authorizes, authenticates and preserves commands with feed back data as TRAC software program and proprietary to this technology and this inventions nature and scope.

46. (NEW) A claim is made according to claim 37, that TRAC software is provided at least a non volatile event memory storage for TRAC event data processed and that it is in secure environments so that it is highly tamper resistant through physical means and equally protected through electrical means and tamper resistant software programming to become an agreed upon in any standards effort for accountable reliable and trusted software commands and record keeping for passive and aggressive remote control and robotics to analyze, judge, evaluate, value, appraise and monitor, manage and control, Vehicle use Machine use, Equipment use, Facility or installation functions, personal use on a person or as a free standing device, to perform; financial transactions in real time and in stationary and mobile settings security checks on components, PFNS and host piece of equipment. Activities through automated controls and actuators retrieval and processing of data from feed back sensors retrieval and processing data from environmental sensors any arbitrary processing, encoding –decoding encrypting-decrypting, modulation demodulation of any electrical, signals both analog and digital in any language, format or protocol.

47. (NEW) A claim is made according to claim 37 as proprietary PFN/TRAC software to provide any data to at least one remote location including, any Ethernet or Intranet and or including any wire or wireless IP gateways (PFNS or other) to provide data to E-mail addresses or web sites through the World Wide Web or Internet for financial Transactions or purposes, governmental or public information or safety uses, tracking and telemetry purpose or for any arbitrary service provider use, social purposes, environmental purposes, individual purpose or use and or any undetermined purposes or use.

48. (NEW) In accordance with claim 37, a further claim is made according to claim two to consider as Proprietary TRAC software protocols with or without this technology's proprietary protected primary focal node or PFN's physical architecture any form of local communication, location equipment and control interface system that reports to a remote location.

49. (NEW) A further claim is made according to claim 37 for the PFN/TRAC system to be inclusive of any industry standard or certification or endorsement by the insurance industry, government agencies, professional organizations, the general public safety and civil rights groups or commercial interest groups, or industry and commercial research groups or trade organizations regarding legally acceptable data storage or accountable remote control for financial transaction products or for any of the specifications detailed for society and it's institutions to be with in the nature and scope of this invention and be proprietary.

50. (NEW) A claim is made for TRAC software record keeping to require terminal and or device electrical serial numbers and personal identification numbers as part of it's authorization and authentication program with the time date any geographic location coordinates or address of all the equipment component and systems participating and or performing entries and or

accessing any application event to be on file in storage on location or remotely to be proprietary to this invention.

51. (NEW) A separate claim is made for an electrical seal system to detect tampering and to provide a water resistant seal protection for any containment for adhering any two surfaces with sophisticated authorization energizing systems without sophisticated authorization energizing systems web page Internet data.

52. (NEW) A separate claim is made for a universal communication interface to perform routing functions, repeater and or digitpeating of RF, wire or wireless telephony, paging light communication, sound or voice recognition technology through a processing interface termed a PFN as part of any standard effort or as an independent multi- tasking communication system.

53. (NEW) According to claim 37 an additional claim is made for a multi frequency scanning transceiver and processor to locate and process any type of wireless communication or wire com link and to process and identify the signals nature and purpose and pass it on in the most efficient pre-programmed manner, to it's final destination and reroute or reconfigure the signal in any available communication format.

54. (NEW) A claim is made for memory of any data processed through the TRAC system in any PFN to have a local memory and redundant remote memory as determined appropriate for any application specific PFN.

55. (NEW) A claim is made for any PFN system to provide data, telemetry, or tracking to a private monitoring and control system, a public system or Internet web site, a commercial web page or e-mail site a privately owned TV and or software program system, e.g., video game, a web TV connectable system e.g., cable or satellite with a joint venture with TV servers and Internet protocol Provider.

56. (NEW) A claim is made for accountable remote control of actuators through the PFN processor.

57. (NEW) A claim is made for accountability of activity controls confirmed by feedback sensors.

58. (NEW) A claim is made for application specific sensing and supplying that data to any form of monitoring or management system through TV computers other PFN devices or other interface arbitrary systems.

59. (NEW) A claim is made for an Intra net system to serve as an interactive highway using a PFN to process and make accountable remote control and robotics for land vehicles.

60. (NEW) And additional claim is made in accordance with claim 37 for the use of specialized policing tools laser gun communication other forms of wireless communication device or even employing TOW missile technology to make contact with an illegal and unauthorized vehicle and to perform a stop or slow stop and secure procedure of the vehicle.

61. (NEW) An additional claim is made according to claim 37 for event memory storage of this event and any application specific event as prescribed by preprogramming or as a result of an authorized remote command.

62. (NEW) A claim is made for the interfacing or up linking of remote monitor or management systems to create larger intra nets or to interface with the Internet with or without encryption.

63. (NEW) A claim is made for the PFN/TRAC system to provide communication switching or repeating or digitpeating automatically or through remote or local commands manually or preprogrammed as protocols.

64. (NEW) A further claim is made according to claim 37 for the local tracking of these communication strings to better locate and make accountable all command data the activities they command and the confirmation of the activity.

65. (NEW) A claim is made for the PFN/TRAC system to incorporate and interface with all machine messaging networks and computer networks private commercial and governmental in an organized system designed by standards and protocols.

66. (NEW) A claim is made for a national registry to track and identify all pieces of equipment and components and to authorize their use, tax and or appraise their impact on society's infrastructure and environment.

67. (NEW) A claim according to claim 37 is made for government agencies national local and world, individuals and commercial interest, and organizations to interact and have special access and Identification.

68. (NEW) A claim according to claim 37 is made for this national registry system for the tracking of stolen parts components, devices and total products or product systems.

69. (NEW) A claim is made for the PFN/TRAC system to be provided as any standards effort prescribes this technology to provide a local organizational electrical interface platform to perform accountable remote control and robotics.

70. (NEW) A further claim is made in accordance with claim 37 for the future up linking of machine messaging networks and computer networks as a PFN/TRAC system determined to make all persons and machinery accountable for their interaction through component FACT identification and recorded communication strings in redundant locations.

71. (NEW) A further claim is made for the spider eyes program and multitasking law enforcement tool to shut down a vehicle through real-time discrimination and identification of equipment and all individuals involved in any event and to provide account ability in all locations in real time, locally in subject vehicle as well as in the police cruiser or memory storage

device, and at any local police dispatch, and also in state police monitoring system and nationally at the FBI or justice dept.

72. (NEW) A further claim according to claim 37 is made for the PFN/TRAC system to provide the means to administer and create a track able record of any such shut down no mater what the means used to deactivate a subject vehicle being operated in an unauthorized or unsafe manner as determined by law, any standards effort, and involving any civil liberties or civil watch dog group.

73. (NEW) A claim is made for automated and remote-controlled communication routing of wireless or land line to and including fiber optic technology through transmission connectables, switches, computer processors, and TRAC programming in the Primary Focal Node, as part of a repeating function for radio frequency digitpeating, wireless telephony, wire and fiberoptics to increase both land line, and wireless service inexpensively through existing or reduced land line wireless and fiber optic hardware.

74. (NEW) A claim is made for TRAC/FACT programming and hardware system to interconnect all communication intranets for government, military, rail, sea, aviation, commercial, agricultural, law enforcement, EPA, etc., including commercial servers and providers through the TRAC/FACT protocol.

75. (NEW) A claim is made for the PFN/TRAC System and functions in accordance with claim 1, to be consolidated and integrated on a chip, as sets of Systems On a Chip (SOC).

76. (NEW) A claim according to claim 33 is made where in, any standard that dedicates any frequencies for communication for remote control or wireless machine messaging, for mobile applications, portable or personal communicating devices, that employ any scanning, process and or rerouting, repeating digipeating, transcribing through high applications and re-transmitting, on other frequency process, and optionally maintains a traceable record.

Appendix D
(complete list of pending claims)

1. A real-time vehicle or equipment management system including a primary focal node (PFN), comprising:

at least one sensory device monitoring and reporting on data including command function results of at least one of peripheral devices and equipment with application specific data and optional application specific geographic coordinates corresponding to the application specific data;

at least one memory, operatively connected to said at least one sensory device, and located in or on the vehicle or the equipment, storing a plurality of interface protocols for interfacing and communicating, said memory equipped with at least one of an application specific backup device and a redundant memory function recording application specific automated and remote control command strings to the peripheral devices that perform automated and remote control functions;

at least one processor responsively connectable to said at least one memory, and implementing the plurality of interface protocols for interfacing and communicating with the plurality of external devices;

a plurality of external devices supported by at least one interface for C.O.T.S. products and accessories, the plurality of external devices interfacing with said at least one processor via at least one of the plurality of interface protocols, including at least one of: pagers, wireless phones, radio frequency equipment, locating equipment systems, cordless phones, laptops, one-way communication device, two-way communication device, and computer organizers, at least one of said plurality of external devices including a report back capability to report the data collected by said at least one sensory device to at least one remote location including the application specific data that is stored in the PFN; and

at least one two-way communication system including at least one security device or routine to condition the signal with at least one security protocol including at least one encryption technology to securely interface between at least one of the plurality of external devices and said at least one processor,

wherein said at least one processor comprises at least a local Primary Focal Node termed a PFN to have hardware and programmable and or modular software or firmware termed TRAC which functions as a Trusted Remote Activity Controller providing robotics or automated and remote control accountability by recording event data local and redundantly in remote memory storage, for communication components and computer hardware systems as determined by any industry or government standards efforts and protocols, for interfacing with activity controls, sensors, or discretes in any vehicle, machine, or as part of any equipment or on any person, animal, living entity or for any arbitrary use as a free standing piece of accountable telemetry or control equipment.

2. A real-time vehicle or equipment management system including an optional security function that restricts unauthorized access thereto, comprising:
at least one operation sensor recording the operations of the at least one of the vehicle and equipment as a recording signal;

a memory storing the operations of the vehicle or the equipment received from said operation sensor in a secure manner; and

a processor responsively connectable to said memory, receiving the recording signal, at least one communication device reporting or transferring data to at least one remote monitoring and control system with transmission of the data being optionally two-way transmission for memory storage recording of remote control commands, the recording signal from at least one of operation sensor, audio data records and visual data records, said at least one communication device comprising at least one of:

a two-way pager responsively connectable via at least one of a processor and a computer stored in a secured manner and capable of transmitting data to download to at least one remote monitoring system;

a wireless telephone responsively connectable via the at least one processor and computer stored in a secure manner and capable of transmitting data to download to the at least one remote monitoring system;

a radio frequency transceiver responsively connectable to the at least one processor and computer stored in a secure manner and capable of transmitting data to download to the at least one remote monitoring system;

a physical connector interface port responsively connectable to the at least one processor and computer and at least one of protected, shielded and maintained in a secure manner, and capable of transferring data to download to the at least one remote monitoring system;

an optical light data transmission port responsively connectable to the at least one processor and computer and securely maintained, and capable of transmitting data to download to the at least one remote monitoring system;

a multi-tasking law enforcement device capable, optionally through electronic security protocols, to communicate with the at least one processor and computer and download to the at least one remote location;

at least one processor and computer responsively connectable to at least one memory and at least one auxiliary communication device in a secure manner that can be processed to any other communication device responsibly connectable to the processor or computer to download the data to the at least one remote monitoring system;

at least one processor and computer responsively connectable to a Global Positioning System (GPS) able of transmitting GPS coordinate data protocol to the at least one remote monitoring system;

at least one processor and computer responsively connectable to at least one magnetic card swipe device that can transmit via other communication devices to the at least one remote monitoring system for at least one of billing, debiting and crediting;

at least one processor and computer responsively connectable to at least one of audio and video devices and other communication systems to at least one of guide and control remotely a vehicle;

at least one processor and computer responsively connectable to at least one memory to record at least one of an audio and video signal, and data used to control a vehicle remotely; and

at least one two-way communication system including at least one security device or routine to condition the signal with at least one security protocol including at least one encryption technology to securely interface between at least one communication device and the remote location,

wherein said at least one processor comprises at least a local Primary Focal Node termed a PFN to have hardware and programmable and or modular software or firmware termed TRAC

which functions as a Trusted Remote Activity Controller providing robotics or automated and remote control accountability by recording event data local and redundantly in remote memory storage, for communication components and computer hardware systems as determined by any industry or government standards efforts and protocols, for interfacing with activity controls, sensors, or discretes in any vehicle, machine, or as part of any equipment or on any person, animal, living entity or for any arbitrary use as a free standing piece of accountable telemetry or control equipment.

3. A real-time vehicle or equipment management system according to claim 1, wherein said plurality of external devices includes at least one of: an electrical actuating accessory and at least one peripheral device controlling automated remote control functions utilizing at least one of electricity, compressed air, gases, vacuums, hydraulic and fluid pressure.

4. A real-time vehicle or equipment management system according to claim 1, wherein said plurality of external devices includes at least one of: electro magnets solenoids, motors, mechanical or silicon relays, pistons, cylinders, pumps, valves, adjustable valves pindle valves cables, linkages levers, shifter forks, paws, ratchets, catches, couplers, spring returns, gearing or power transfer mechanisms cases, brake pads disk assemblies, or drums, clutches and/or interlocking drive mechanisms, spined hub collars and shafts.

5. A real-time vehicle or equipment management system according to claim 1, wherein said at least one of said plurality of external devices include a backup system to provide back up to any automated, remote control system.

6. A real-time vehicle or equipment management system according to claim 1, wherein said at least one of said plurality of external devices includes at least one of a coyote circuit and other circuit used to create a plug and play connector as a universal modality to interface with at least one of electrical parts, components, devices, C.O.T.S. personal products or different manufactures products.

7. A real-time vehicle or equipment management system according to claim 1, wherein said at least one of said plurality of external devices includes at least one application used in conjunction with a security system, home computer controller system, household equipment and utilities management system to organize, store, complete phone node contact and transmit data for utility and/or equipment use for any billing, personal records and/or taxing for same, as well as, provide services for repair and maintenance purposes.

8. A real-time vehicle or equipment management system according to claim 1, wherein said at least one of said plurality of external devices includes the function of operating at a specific location and not being transferrable to another location without authorization, and when transferred in an unauthorized manner, the at least one of said plurality of devices transmits an identification signal to report the location of the displaced equipment.

9. A real-time vehicle or equipment management system according to claim 1, wherein said at least one of said plurality of external devices are supported by a universal interface for separate C.O.T.S. products and accessories, the at least one of the plurality of external devices interfacing with said at least one processor via the at least one of the plurality of interface protocols, providing the capability of the at least one of the external devices to be at least one of remotely controlled and remotely operated.

10. A real-time vehicle or equipment management system according to claim 1, wherein said primary focal node supports at least one of application specific software protocols and hardware systems for industry standards for recorded data as determined by at least one of codes, specifications, rules regulations, and laws, for at least one of vehicles, equipment or machinery use.

11. A real-time vehicle or equipment management system according to claim 1, wherein said real-time vehicle or equipment management system includes redundant remote storage in at least one remote location in at least one application specific industry standard protocol as determined by at least one of codes, specifications, rules, regulations, data handling procedures and laws for at least one of equipment, machinery and vehicle use.

12. A real-time vehicle or equipment management system according to claim 1, wherein said real-time vehicle or equipment management system is at least one of global network, web and Internet accessible to monitor remote control function in real time and to mass store data off-board as transmitted by the PFN and/or other machine messaging systems and to access the web for personal use from the PFN for E-mail messaging and/or remote tracking either personally, as commercial service and/or for legal and/or governmental reasons.

13. A real-time vehicle or equipment management system according to claim 1, wherein said real-time vehicle recording system is substantially stored in a stop and control box to prevent unauthorized access thereto and the vehicle.

14. A real-time vehicle or equipment management system according to claim 1, further comprising a payment mechanism in or on the vehicle, responsively connectable to said at least one processor, said payment mechanism collecting vehicle information and providing real-time billing, debiting or crediting from the vehicle, and retrieving at least one of a script or electronic signature from a card carrier, and verifying the identity of the card carrier via at least one of photograph, fingerprints, and identification.

15. A real-time vehicle or equipment management system according to claim 1, wherein said at least one processor performs at least one of the following functions:

remotely controlling at least one of robotic functions to activate and control vehicle operations, remotely billing for use of the vehicle, remotely operating at least one machine, evaluating and diagnosing computer or processor malfunctions, remotely ordering materials and service personnel to perform at least one of service and repairs, remotely performing price quotes for cost of the at least one of service and repairs, remotely performing repairs electronically, and remotely shutting down equipment;

remotely controlling data exchange representing a monetary exchange via a focal node to perform a secure and protected containment function of: to restrict unauthorized use of equipment, to record and preserve data in an acceptable legal manner, and to bill at least the vehicle user, thereby providing a total accountability system;

at least one of networking and communicating with at least one gateway to other computers and computer networks that manage data, said gateway determining whether the other computers and computer networks are to be at least one of networked and communicated with to further monitor and store data for at least one of billing, regulatory compliance and legal compliance, and optionally for at least one of social economic and environmental impact;

at least one of networking and communicating with at least one of other computers and computer networks that manage data, including at least one of vehicle location, equipment technical assistance, personal accounting for machine or equipment use, billing, debiting, crediting, vehicle operations, service and repairs; and

monitoring equipment for health and safety conditions potentially adversely affecting the public, including at least one of reckless driving, driver impairment, pollution, vehicle unsafety.

16. A real-time vehicle or equipment management system according to claim 1, wherein said at least one processor performs at least one of the following functions:

collecting machine message data from said real-time vehicle recording system used to compile data for a public media or web page, and transmitting the machine data thereto;

presenting the machine message data on at least one web page that originated from at least one equipment on said real-time vehicle or from a machine messaging network;

recording and reporting to a monitoring gateway for billing for highway use by the vehicle;

collecting and storing data corresponding to charging at least one electric vehicle;

reporting, recording and billing automatically using a real-time billing system in the vehicle corresponding to time a geographic area roadway is used;

determining impact on environment including roadways, using at least one sensor recording at least one of:

weight and emissions ratings for atmospheric impact type of at least one of fuel and energy used;

time of operational machine use;

amount of fuel or energy used;

type of waste product produced; and

amount of the waste product produced.

17. A real-time vehicle or equipment management system according to claim 1, wherein said at least one processor performs at least one of the following functions:

recording at least one of audio and video traffic vehicle impact, and recording and reporting to at least one remote monitoring system for at least one accident investigation and machine accidents in a data secure manner;

recording information used in insurance investigations to decide claims and assign liability;

determining liability and accountability to be used in legal proceedings and optionally to be used in determining safety parameters, rules, regulations and laws;

recording at least one of audio and video captured criminal incidents by activating unattended vehicle systems to report criminal events through remote control;

recording at least one of audio and video captured news events as witnessed by a machine system including at least one of weather conditions, and traffic conditions.

18. A real-time vehicle or equipment management system according to claim 1, further comprising at least one operations sensor recording information including at least one of operations of the vehicle, highway conditions, speed limits, driving conditions including speeding, reckless driving, drunken driving, road rage, pensive or inefficient driving, and wherein the information of the vehicle are received from said operation sensor and stored in said memory and downloaded to at least one of a remote monitoring system, a remote billing system, and a remote data analysis system.

19. A real-time vehicle or equipment management system according to claim 1, wherein storage of the information includes storage with two onboard and at least one offboard storage of the host piece of equipment, the offboard storage optionally including application specific Email or warning flag detailing an electronic serial number associated with a privately owned or personal E-mail address.

20. A real-time vehicle or equipment management system according to claim 1, wherein the PFN includes more than one purpose optionally billing for commercial service or for specific service of a machine and simultaneously gathering data on any incident or accident event or provide additional controls by off board control and/or management systems in an emergency or in the case of a compromised operator in real-time.

21. A real-time vehicle or equipment management system according to claim 1, wherein an electronic serial number (ESN) allows each element within the matrix to be securely and accurately tracked, inventoried or controlled, either through a local control loop or remotely, by an authorized application or agency.

22. A real-time vehicle or equipment management system according to claim 1, wherein an electronic serial number includes the basis for digital encryption of information passed between the PFN device and the controlling entity with local network processing nodes through public communications channels such as the phone lines or Internet initiated in many cases wirelessly from mobile PFNs accompanied by their Mobile Identification Number.

23. A real-time vehicle or equipment management system according to claim 1, wherein this programmable software and/or any other accountable software program that performs automated and remote control and/or robotics functions as a result of programming that can authorize, authenticate and preserves commands and save feedback data as a TRAC software program and proprietary to this technology and its nature and scope.

24. A real-time vehicle or equipment management system according to claim 1, wherein at least one non-volatile memory storage and controlled events are in secured environments so that it is highly tamper resistant through physical means and equally protected through electrical means and tamper resistant software programming to become an agreed upon standard for accountable

reliable and trusted software commands and record keeping for passive and aggressive remote control and robotics to analyze, judge, evaluate, value, appraise and monitor, manage and control at least one of vehicle use, machine use, equipment use, facility or installation functions, perform financial transactions in real time and in stationary and mobile settings.

25. A real-time vehicle or equipment management system according to claim 1, wherein accountable data is provided to an E-mail address web site and/or through the use of the World Wide Web and/or Internet Protocol (IP) for at least one of financial purposes, government uses, service providers, social purposes, environmental purposes.

26. A real-time vehicle or equipment management system according to claim 1, wherein at least one of modular and programmable routines are determined by the existing hardware and operating system firmware or software for any application responsively connectable through any communication medium by querying each component device attached through a PFN/TRAC system and/or piece of equipment to determine if said connectable component is legitimate and cleared for safe public use.

27. A real-time vehicle or equipment management system according to claim 1, wherein a registry includes all applicable government agencies with their own access to the Registry and/or network with encrypted codes and Identity command strings which are communicative and also access for the general public and their Private Encrypted Identity codes (PINs, etc.) access to same said registry.

28. A real-time vehicle or equipment management system according to claim 1, wherein a registry is accessible by a plurality of manufacturers on a worldwide scale with a plurality of security protocols in the marketing of component, devices and equipment and manufacture must provide a program to be given authorization for sale, and wherein the registry will not activate either the component device and/or piece of equipment without authorization, and resale of the component device or piece of equipment will be requested upon each connectable and queried to respond to the nature of the new install as the registry is contacted and requested to activate the unit.

29. A real-time vehicle or equipment management system according to claim 1, wherein a registry including encryption on the Web will support any and all payment industry software.

31. A real-time vehicle or equipment management system according to claim 1, wherein record keeping requires at least one of terminal and device electrical serial numbers and personal identification numbers as part of its authorization and authentication program with the time date and any geographic location coordinates or address of all the equipment and systems participating or performing entries or accessing any application folder or event file in storage at any location or part of the registry.

32. A real-time vehicle or equipment management system according to claim 1, wherein a host piece of equipment will not operate any of its accessories unless it is provided the correct signal from the registry or a security network, and wherein commercial off the shelf (COTS) products utilize the security functions, resulting in immediate and cost effective conversions.

33. A portable primary focal node (PFN) tracking device that is worn by an individual and reports a location to at least one web address through a public server gateway node, or publicly owned provider node using any type of communication system, an additional claim is made for the networking use of any multi-communication capable PFN to relay or repeat shorter range signals for personally worn PFN devices, wherein said PFN includes hardware and programmable and or modular software or firmware termed TRAC which functions as a Trusted Remote Activity Controller providing robotics or automated and remote control accountability by recording event data local and redundantly in remote memory storage, for communication components and computer hardware systems as determined by any industry or government standards efforts and protocols, for interfacing with activity controls, sensors, or discretes in any vehicle, machine, or as part of any equipment or on any person, animal, living entity or for any arbitrary use as a free standing piece of accountable telemetry or control equipment.

34. A real-time or equipment management system according to claim 1 that serves as an accountable end user instruction center or audio tutor to deliver E-learning and educational programming via the PFN TRAC System and discretes.

35. A real-time or equipment management system according to claim 1 that can be converted to the highest government and military security protocols, e.g., DES and DET, for national security public safety, nation briefing functions.

36. A real-time or equipment management system according to claim 1 that provides write one-time memory storage locally as a secure accountable function to track and identify the source of any tampering or hacking to the PFN/TRAC System.

37. A claim is made for a local Primary Focal Node termed a PFN to have hardware and programmable and or modular software or firmware termed TRAC which functions as a Trusted Remote Activity Controller providing robotics or automated and remote control accountability by recording event data local and redundantly in remote memory storage, for communication components and computer hardware systems as determined by any industry or government standards efforts and protocols, for interfacing with activity controls, sensors, or discretes in any vehicle, machine, or as part of any equipment or on any person, animal, living entity or for any arbitrary use as a free standing piece of accountable telemetry or control equipment.

38. An additional claim is made for a connectable system software termed TRACS to be operational with the PFN/TRAC local devices and capable of receiving PFN routing of the numerous sub programs and the application specific data strings as detailed in all PFN application specifications and creating a secure redundant event memory storage.

39. An additional claim to claim 37 is made for the entire system to provide accurate records of operation and failure as determined by a standards effort to be considered a Trusted system.

40. A further claim is made according to claim 37 for any fail safe or backup system necessary to be qualified as a trusted device and system as determined by any standards effort at any time in the future.

41. A claim is made according to claim 37 that this software and hardware be in a protective encasement application specific to it's environment and purpose and also to be determined by any standards effort at any time in the future.

42. A claim is a made according to claim 37 that the software and hardware have no special encasement provision. and can be constructed in any functional configuration and format.

43. A claim is made according to claim 37 for an electric certified seal mechanism to secure any encased area and to determine if the area has been breached; this device and system is also to be determined by any stands effort or law.

44. A claim is made according to claim 37 for a mechanical locking device or system to secure any encased area.

45. A claim is made according to claim 37 to refer to this modular and programmable software program or any other programming that performs automated accountable remote control and or robotics functions that authorizes, authenticates and preserves commands with feed back data as TRAC software program and proprietary to this technology and this inventions nature and scope.

46. A claim is made according to claim 37, that TRAC software is provided at least a non volatile event memory storage for TRAC event data processed and that it is in secure environments so that it is highly tamper resistant through physical means and equally protected through electrical means and tamper resistant software programming to become an agreed upon in any standards effort for accountable reliable and trusted software commands and record keeping for passive and aggressive remote control and robotics to analyze, judge, evaluate, value, appraise and monitor, manage and control, Vehicle use Machine use, Equipment use, Facility or installation functions, personal use on a person or as a free standing device, to perform; financial transactions in real time and in stationary and mobile settings security checks on components, PFNS and host piece of equipment. Activities through automated controls and actuators retrieval and processing of data from feed back sensors retrieval and processing data from environmental sensors any arbitrary processing, encoding –decoding encrypting-decrypting, modulation demodulation of any electrical, signals both analog and digital in any language, format or protocol.

47. A claim is made according to claim 37 as proprietary PFN/TRAC software to provide any data to at least one remote location including, any Ethernet or Intranet and or including any wire or wireless IP gateways (PFNS or other) to provide data to E-mail addresses or web sites through the World Wide Web or Internet for financial Transactions or purposes, governmental or public information or safety uses, tracking and telemetry purpose or for any arbitrary service provider use, social purposes, environmental purposes, individual purpose or use and or any undetermined purposes or use.

48. In accordance with claim 37, a further claim is made according to claim two to consider as Proprietary TRAC software protocols with or without this technology's proprietary protected

primary focal node or PFN's physical architecture any form of local communication, location equipment and control interface system that reports to a remote location.

49. A further claim is made according to claim 37 for the PFN/TRAC system to be inclusive of any industry standard or certification or endorsement by the insurance industry, government agencies, professional organizations, the general public safety and civil rights groups or commercial interest groups, or industry and commercial research groups or trade organizations regarding legally acceptable data storage or accountable remote control for financial transaction products or for any of the specifications detailed for society and it's institutions to be with in the nature and scope of this invention and be proprietary.

50. A claim is made for TRAC software record keeping to require terminal and or device electrical serial numbers and personal identification numbers as part of it's authorization and authentication program with the time date any geographic location coordinates or address of all the equipment component and systems participating and or performing entries and or accessing any application event to be on file in storage on location or remotely to be proprietary to this invention.

51. A separate claim is made for an electrical seal system to detect tampering and to provide a water resistant seal protection for any containment for adhering any two surfaces with sophisticated authorization energizing systems without sophisticated authorization energizing systems web page Internet data.

52. A separate claim is made for a universal communication interface to perform routing functions, repeater and or digitpeating of RF, wire or wireless telephony, paging light communication, sound or voice recognition technology through a processing interface termed a PFN as part of any standard effort or as an independent multi- tasking communication system.

53. According to claim 37 an additional claim is made for a multi frequency scanning transceiver and processor to locate and process any type of wireless communication or wire com link and to process and identify the signals nature and purpose and pass it on in the most efficient pre-programmed manner, to it's final destination and reroute or reconfigure the signal in any available communication format.

54. A claim is made for memory of any data processed through the TRAC system in any PFN to have a local memory and redundant remote memory as determined appropriate for any application specific PFN.

55. A claim is made for any PFN system to provide data, telemetry, or tracking to a private monitoring and control system, a public system or Internet web site, a commercial web page or e-mail site a privately owned TV and or software program system, e.g., video game, a web TV connectable system e.g., cable or satellite with a joint venture with TV servers and Internet protocol Provider.

56. A claim is made for accountable remote control of actuators through the PFN processor.

57. A claim is made for accountability of activity controls confirmed by feedback sensors.

58. A claim is made for application specific sensing and supplying that data to any form of monitoring or management system through TV computers other PFN devices or other interface arbitrary systems.

59. A claim is made for an Intra net system to serve as an interactive highway using a PFN to process and make accountable remote control and robotics for land vehicles.

60. And additional claim is made in accordance with claim 37 for the use of specialized policing tools laser gun communication other forms of wireless communication device or even employing TOW missile technology to make contact with an illegal and unauthorized vehicle and to perform a stop or slow stop and secure procedure of the vehicle.

61. An additional claim is made according to claim 37 for event memory storage of this event and any application specific event as prescribed by preprogramming or as a result of an authorized remote command.

62. A claim is made for the interfacing or up linking of remote monitor or management systems to create larger intra nets or to interface with the Internet with or without encryption.

63. A claim is made for the PFN/TRAC system to provide communication switching or repeating or digitpeating automatically or through remote or local commands manually or preprogrammed as protocols.

64. A further claim is made according to claim 37 for the local tracking of these communication strings to better locate and make accountable all command data the activities they command and the confirmation of the activity.

65. A claim is made for the PFN/TRAC system to incorporate and interface with all machine messaging networks and computer networks private commercial and governmental in an organized system designed by standards and protocols.

66. A claim is made for a national registry to track and identify all pieces of equipment and components and to authorize their use, tax and or appraise their impact on society's infrastructure and environment.

67. A claim according to claim 37 is made for government agencies national local and world, individuals and commercial interest, and organizations to interact and have special access and Identification.

68. A claim according to claim 37 is made for this national registry system for the tracking of stolen parts components, devices and total products or product systems.

69. A claim is made for the PFN/TRAC system to be provided as any standards effort prescribes this technology to provide a local organizational electrical interface platform to perform accountable remote control and robotics.

70. A further claim is made in accordance with claim 37 for the future up linking of machine messaging networks and computer networks as a PFN/TRAC system determined to make all persons and machinery accountable for their interaction through component FACT identification and recorded communication strings in redundant locations.

71. A further claim is made for the spider eyes program and multitasking law enforcement tool to shut down a vehicle through real-time discrimination and identification of equipment and all individuals involved in any event and to provide account ability in all locations in real time, locally in subject vehicle as well as in the police cruiser or memory storage device, and at any local police dispatch, and also in state police monitoring system and nationally at the FBI or justice dept.

72. A further claim according to claim 37 is made for the PFN/TRAC system to provide the means to administer and create a track able record of any such shut down no mater what the means used to deactivate a subject vehicle being operated in an unauthorized or unsafe manner as determined by law, any standards effort, and involving any civil liberties or civil watch dog group.

73. A claim is made for automated and remote-controlled communication routing of wireless or land line to and including fiber optic technology through transmission connectables, switches, computer processors, and TRAC programming in the Primary Focal Node, as part of a repeating function for radio frequency digitpeating, wireless telephony, wire and fiberoptics to increase both land line, and wireless service inexpensively through existing or reduced land line wireless and fiber optic hardware.

74. A claim is made for TRAC/FACT programming and hardware system to interconnect all communication intranets for government, military, rail, sea, aviation, commercial, agricultural, law enforcement, EPA, etc., including commercial servers and providers through the TRAC/FACT protocol.

75. A claim is made for the PFN/TRAC System and functions in accordance with claim 1 to be consolidated and integrated on a chip, as sets of Systems On a Chip (SOC).

76. A claim according to claim 33 is made where in, any standard that dedicates any frequencies for communication for remote control or wireless machine messaging, for mobile applications, portable or personal communicating devices, that employ any scanning, process and or rerouting, repeating digipeating, transcribing through high applications and re-transmitting, on other frequency process, and optionally maintains a traceable record.

Docket No.: 110273.500US1

PATENT/**OFFICIAL**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	
Richard C. WALKER	:	
Serial No. unassigned	:	Group Art Unit: unassigned
Filed: herewith	:	Examiner: unassigned

For: SECURE, ACCOUNTABLE, MODULAR AND PROGRAMMABLE SOFTWARE TRAC

PRELIMINARY AMENDMENT

Honorable Commissioner for Patents
Washington, D. C. 20231

Sir:

This Preliminary Amendment is being filed concurrently with the above-referenced application. The following amendments and remarks are respectfully submitted.

IN THE CLAIMS

Please cancel claims 21-75 and without prejudice or disclaimer.

Please amend claims 3-20 as indicated in the attached Appendix A. A complete set of claims is attached in Appendix B.

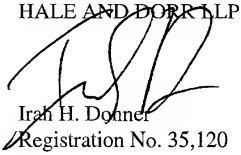
REMARKS

This Preliminary Amendment is submitted to improve the form of the specification and claims as originally filed. The Related Applications Section has been corrected to more appropriately claim priority and continuation status. It is respectfully requested that this Preliminary Amendment be favorably examined and entered in the above-referenced application.

AUTHORIZATION

The Commissioner is hereby authorized to charge any additional fees which may be required for this Amendment, or credit any overpayment to deposit account no. 08-0219. In the event that an extension of time is required, or which may be required in addition to that requested in a petition for an extension of time, the Commissioner is requested to grant a petition for that extension of time which is required to make this response timely and is hereby authorized to charge any fee for such an extension of time or credit any overpayment for an extension of time to deposit account no. 08-0219.

Respectfully submitted,
HALE AND DORR LLP



Iran H. Donner
Registration No. 35,120

1455 Pennsylvania Avenue, N.W.
Washington, DC 20004-1008
(202) 942-8400
Date: 12/19/01
IHD/sed

Appendix A
(amended claims)

3. (ONCE AMENDED) A real-time vehicle or equipment management system according to claim[s] 1 [or 2], wherein said plurality of external devices includes at least one of: an electrical actuating accessory and at least one peripheral device controlling automated remote control functions utilizing at least one of electricity, compressed air, gases, vacuums, hydraulic and fluid pressure.

4. (ONCE AMENDED) A real-time vehicle or equipment management system according to claim[s] 1 [or 2], wherein said plurality of external devices includes at least one of: electro magnets solenoids, motors, mechanical or silicon relays, pistons, cylinders, pumps, valves, adjustable valves pindle valves cables, linkages levers, shifter forks, paws, ratchets, catches, couplers, spring returns, gearing or power transfer mechanisms cases, brake pads disk assemblies, or drums, clutches and/or interlocking drive mechanisms, spined hub collars and shafts.

5. (ONCE AMENDED) A real-time vehicle or equipment management system according to claim[s] 1 [or 2], wherein said at least one of said plurality of external devices include a backup system to provide back up to any automated, remote control system.

6. (ONCE AMENDED) A real-time vehicle or equipment management system according to claim[s] 1 [or 2], wherein said at least one of said plurality of external devices includes at least one of a coyote circuit and other circuit used to create a plug and play connector as a universal modality to interface with at least one of electrical parts, components, devices, C.O.T.S. personal products or different manufactures products.

7. (ONCE AMENDED) A real-time vehicle or equipment management system according to claim[s] 1 [or 2], wherein said at least one of said plurality of external devices includes at least one application used in conjunction with a security system, home computer controller system, household equipment and utilities management system to organize, store, complete phone node contact and transmit data for utility and/or equipment use for any billing, personal records and/or taxing for same, as well as, provide services for repair and maintenance purposes.

8. (ONCE AMENDED) A real-time vehicle or equipment management system according to claim[s] 1 [or 2], wherein said at least one of said plurality of external devices includes the function of operating at a specific location and not being transferrable to another location without authorization, and when transferred in an unauthorized manner, the at least one of said plurality of devices transmits an identification signal to report the location of the displaced equipment.

9. (ONCE AMENDED) A real-time vehicle or equipment management system according to claim[s] 1 [or 2], wherein said at least one of said plurality of external devices are supported by a universal interface for separate C.O.T.S. products and accessories, the at least one of the plurality of external devices interfacing with said at least one processor via the at least one of the plurality of interface protocols, providing the capability of the at least one of the external devices to be at least one of remotely controlled and remotely operated.

10. (ONCE AMENDED) A real-time vehicle or equipment management system according to claim[s] 1 [or 2], wherein said primary focal node supports at least one of application specific software protocols and hardware systems for industry standards for recorded data as determined by at least one of codes, specifications, rules regulations, and laws, for at least one of vehicles, equipment or machinery use.

11. (ONCE AMEDNED) A real-time vehicle or equipment management system according to claim[s]1 [or 2], wherein said real-time vehicle or equipment management system includes redundant remote storage in at least one remote location in at least one application specific industry standard protocol as determined by at least one of codes, specifications, rules, regulations, data handling procedures and laws for at least one of equipment, machinery and vehicle use.

12. (ONCE AMENDED) A real-time vehicle or equipment management system according to claim[s] 1 [or 2], wherein said real-time vehicle or equipment management system is at least one of global network, web and Internet accessible to monitor remote control function in real time and to mass store data off-board as transmitted by the PFN and/or other machine messaging systems and to access the web for personal use from the PFN for E-mail messaging and/or remote tracking either personally, as commercial service and/or for legal and/or governmental reasons.

13. (ONCE AMENDED) A real-time vehicle or equipment management system according to claim[s] 1 [or 2], wherein said real-time vehicle recording system is substantially stored in a stop and control box to prevent unauthorized access thereto and the vehicle.

14. (ONCE AMENDED) A real-time vehicle or equipment management system according to claim[s] 1 [or 2], further comprising a payment mechanism in or on the vehicle, responsively connectable to said at least one processor, said payment mechanism collecting vehicle information and providing real-time billing, debiting or crediting from the vehicle, and retrieving at least one of a script or electronic signature from a card carrier, and verifying the identity of the card carrier via at least one of photograph, fingerprints, and identification.

15. (ONCE AMENDED) A real-time vehicle or equipment management system according to claim[s] 1 [or 2], wherein said at least one processor performs at least one of the following functions:

remotely controlling at least one of robotic functions to activate and control vehicle operations, remotely billing for use of the vehicle, remotely operating at least one machine, evaluating and diagnosing computer or processor malfunctions, remotely ordering materials and service personnel to perform at least one of service and repairs, remotely performing price quotes for cost of the at least one of service and repairs, remotely performing repairs electronically, and remotely shutting down equipment;

remotely controlling data exchange representing a monetary exchange via a focal node to perform a secure and protected containment function of: to restrict unauthorized use of equipment, to record and preserve data in an acceptable legal manner, and to bill at least the vehicle user, thereby providing a total accountability system;

at least one of networking and communicating with at least one gateway to other computers and computer networks that manage data, said gateway determining whether the other computers and computer networks are to be at least one of networked and communicated with to further monitor and store data for at least one of billing, regulatory compliance and legal compliance, and optionally for at least one of social economic and environmental impact;

at least one of networking and communicating with at least one of other computers and computer networks that manage data, including at least one of vehicle location, equipment technical assistance, personal accounting for machine or equipment use, billing, debiting, crediting, vehicle operations, service and repairs; and

monitoring equipment for health and safety conditions potentially adversely affecting the public, including at least one of reckless driving, driver impairment, pollution, vehicle unsafety.

16. (ONCE AMENDED) A real-time vehicle or equipment management system according to claim[s] 1 [or 2], wherein said at least one processor performs at least one of the following functions:

collecting machine message data from said real-time vehicle recording system used to compile data for a public media or web page, and transmitting the machine data thereto;

presenting the machine message data on at least one web page that originated from at least one equipment on said real-time vehicle or from a machine messaging network;

recording and reporting to a monitoring gateway for billing for highway use by the vehicle;

collecting and storing data corresponding to charging at least one electric vehicle;

reporting, recording and billing automatically using a real-time billing system in the vehicle corresponding to time a geographic area roadway is used;

determining impact on environment including roadways, using at least one sensor recording at least one of:

weight and emissions ratings for atmospheric impact type of at least one of fuel and energy used;

time of operational machine use;

amount of fuel or energy used;

type of waste product produced; and

amount of the waste product produced.

17. (ONCE AMENDED) A real-time vehicle or equipment management system according to claim[s] 1 [or 2], wherein said at least one processor performs at least one of the following functions:

recording at least one of audio and video traffic vehicle impact, and recording and reporting to at least one remote monitoring system for at least one accident investigation and machine accidents in a data secure manner;

recording information used in insurance investigations to decide claims and assign liability;

determining liability and accountability to be used in legal proceedings and optionally to be used in determining safety parameters, rules, regulations and laws;

recording at least one of audio and video captured criminal incidents by activating unattended vehicle systems to report criminal events through remote control;

recording at least one of audio and video captured news events as witnessed by a machine system including at least one of weather conditions, and traffic conditions.

18. (ONCE AMENDED) A real-time vehicle or equipment management system according to claim[s] 1 [or 2], further comprising at least one operations sensor recording information including at least one of operations of the vehicle, highway conditions, speed limits, driving conditions including speeding, reckless driving, drunken driving, road rage, pensive or inefficient driving, and wherein the information of the vehicle are received from said operation sensor and stored in said memory and downloaded to at least one of a remote monitoring system, a remote billing system, and a remote data analysis system.

19. (ONCE AMENDED) A real-time vehicle or equipment management system according to claim[s] 1 [or 2], wherein storage of the information includes storage with two onboard and at least one offboard storage of the host piece of equipment, the offboard storage optionally including application specific Email or warning flag detailing an electronic serial number associated with a privately owned or personal E-mail address.

20. (ONCE AMENDED) A real-time vehicle or equipment management system according to claim[s] 1 [or 2], wherein the PFN includes more than one purpose optionally billing for commercial service or for specific service of a machine and simultaneously gathering data on any incident or accident event or provide additional controls by off board control and/or management systems in an emergency or in the case of a compromised operator in real-time.

Appendix B
(complete set of pending claims)

1. A real-time vehicle or equipment management system including a primary focal node (PFN), comprising:

at least one sensory device monitoring and reporting on data including command function results of at least one of peripheral devices and equipment with application specific data and optional application specific geographic coordinates corresponding to the application specific data;

at least one memory, operatively connected to said at least one sensory device, and located in or on the vehicle or the equipment, storing a plurality of interface protocols for interfacing and communicating, said memory equipped with at least one of an application specific backup device and a redundant memory function recording application specific automated and remote control command strings to the peripheral devices that perform automated and remote control functions;

at least one processor responsively connectable to said at least one memory, and implementing the plurality of interface protocols for interfacing and communicating with the plurality of external devices;

a plurality of external devices supported by at least one interface for C.O.T.S. products and accessories, the plurality of external devices interfacing with said at least one processor via at least one of the plurality of interface protocols, including at least one of: pagers, wireless phones, radio frequency equipment, locating equipment systems, cordless phones, laptops, one-way communication device, two-way communication device, and computer organizers, at least one of said plurality of external devices including a report back capability to report the data collected by said at least one sensory device to at least one remote location including the application specific data that is stored in the PFN; and

at least one two-way communication system including at least one security device or routine to condition the signal with at least one security protocol including at least one encryption technology to securely interface between at least one of the plurality of external devices and said at least one processor,

wherein said at least one processor comprises at least a local Primary Focal Node termed a PFN to have hardware and programmable and or modular software or firmware termed TRAC which functions as a Trusted Remote Activity Controller providing robotics or automated and remote control accountability by recording event data local and redundantly in remote memory storage, for communication components and computer hardware systems as determined by any industry or government standards efforts and protocols, for interfacing with activity controls, sensors, or discretes in any vehicle, machine, or as part of any equipment or on any person, animal, living entity or for any arbitrary use as a free standing piece of accountable telemetry or control equipment.

2. A real-time vehicle or equipment management system including an optional security function that restricts unauthorized access thereto, comprising:

at least one operation sensor recording the operations of the at least one of the vehicle and equipment as a recording signal;

a memory storing the operations of the vehicle or the equipment received from said operation sensor in a secure manner; and

a processor responsively connectable to said memory, receiving the recording signal, at least one communication device reporting or transferring data to at least one remote monitoring and control system with transmission of the data being optionally two-way transmission for memory storage recording of remote control commands, the recording signal from at least one of operation sensor, audio data records and visual data records, said at least one communication device comprising at least one of:

a two-way pager responsively connectable via at least one of a processor and a computer stored in a secured manner and capable of transmitting data to download to at least one remote monitoring system;

a wireless telephone responsively connectable via the at least one processor and computer stored in a secure manner and capable of transmitting data to download to the at least one remote monitoring system;

a radio frequency transceiver responsively connectable to the at least one processor and computer stored in a secure manner and capable of transmitting data to download to the at least one remote monitoring system;

a physical connector interface port responsively connectable to the at least one processor and computer and at least one of protected, shielded and maintained in a secure manner, and capable of transferring data to download to the at least one remote monitoring system;

an optical-light data transmission port responsively connectable to the at least one processor and computer and securely maintained, and capable of transmitting data to download to the at least one remote monitoring system;

a multi-tasking law enforcement device capable, optionally through electronic security protocols, to communicate with the at least one processor and computer and download to the at least one remote location;

at least one processor and computer responsively connectable to at least one memory and at least one auxiliary communication device in a secure manner that can be processed to any other communication device responsibly connectable to the processor or computer to download the data to the at least one remote monitoring system;

at least one processor and computer responsively connectable to a Global Positioning System (GPS) able of transmitting GPS coordinate data protocol to the at least one remote monitoring system;

at least one processor and computer responsively connectable to at least one magnetic card swipe device that can transmit via other communication devices to the at least one remote monitoring system for at least one of billing, debiting and crediting;

at least one processor and computer responsively connectable to at least one of audio and video devices and other communication systems to at least one of guide and control remotely a vehicle;

at least one processor and computer responsively connectable to at least one memory to record at least one of an audio and video signal, and data used to control a vehicle remotely; and

at least one two-way communication system including at least one security device or routine to condition the signal with at least one security protocol including at least one encryption technology to securely interface between at least one communication device and the remote location,

wherein said at least one processor comprises at least a local Primary Focal Node termed a PFN to have hardware and programmable and or modular software or firmware termed TRAC

which functions as a Trusted Remote Activity Controller providing robotics or automated and remote control accountability by recording event data local and redundantly in remote memory storage, for communication components and computer hardware systems as determined by any industry or government standards efforts and protocols, for interfacing with activity controls, sensors, or discretes in any vehicle, machine, or as part of any equipment or on any person, animal, living entity or for any arbitrary use as a free standing piece of accountable telemetry or control equipment.

3. A real-time vehicle or equipment management system according to claim 1, wherein said plurality of external devices includes at least one of: an electrical actuating accessory and at least one peripheral device controlling automated remote control functions utilizing at least one of electricity, compressed air, gases, vacuums, hydraulic and fluid pressure.

4. A real-time vehicle or equipment management system according to claim 1, wherein said plurality of external devices includes at least one of: electro magnets solenoids, motors, mechanical or silicon relays, pistons, cylinders, pumps, valves, adjustable valves pindle valves cables, linkages levers, shifter forks, paws, ratchets, catches, couplers, spring returns, gearing or power transfer mechanisms cases, brake pads disk assemblies, or drums, clutches and/or interlocking drive mechanisms, spined hub collars and shafts.

5. A real-time vehicle or equipment management system according to claim 1, wherein said at least one of said plurality of external devices include a backup system to provide back up to any automated, remote control system.

6. A real-time vehicle or equipment management system according to claim 1, wherein said at least one of said plurality of external devices includes at least one of a coyote circuit and other circuit used to create a plug and play connector as a universal modality to interface with at least one of electrical parts, components, devices, C.O.T.S. personal products or different manufactures products.

7. A real-time vehicle or equipment management system according to claim 1, wherein said at least one of said plurality of external devices includes at least one application used in conjunction with a security system, home computer controller system, household equipment and utilities management system to organize, store, complete phone node contact and transmit data for utility and/or equipment use for any billing, personal records and/or taxing for same, as well as, provide services for repair and maintenance purposes.

8. A real-time vehicle or equipment management system according to claim 1, wherein said at least one of said plurality of external devices includes the function of operating at a specific location and not being transferrable to another location without authorization, and when transferred in an unauthorized manner, the at least one of said plurality of devices transmits an identification signal to report the location of the displaced equipment.

9. A real-time vehicle or equipment management system according to claim 1, wherein said at least one of said plurality of external devices are supported by a universal interface for separate C.O.T.S. products and accessories, the at least one of the plurality of external devices interfacing with said at least one processor via the at least one of the plurality of interface protocols, providing the capability of the at least one of the external devices to be at least one of remotely controlled and remotely operated.

10. A real-time vehicle or equipment management system according to claim 1, wherein said primary focal node supports at least one of application specific software protocols and hardware systems for industry standards for recorded data as determined by at least one of codes, specifications, rules regulations, and laws, for at least one of vehicles, equipment or machinery use.

11. A real-time vehicle or equipment management system according to claim 1, wherein said real-time vehicle or equipment management system includes redundant remote storage in at least one remote location in at least one application specific industry standard protocol as determined by at least one of codes, specifications, rules, regulations, data handling procedures and laws for at least one of equipment, machinery and vehicle use.

12. A real-time vehicle or equipment management system according to claim 1, wherein said real-time vehicle or equipment management system is at least one of global network, web and Internet accessible to monitor remote control function in real time and to mass store data off-board as transmitted by the PFN and/or other machine messaging systems and to access the web for personal use from the PFN for E-mail messaging and/or remote tracking either personally, as commercial service and/or for legal and/or governmental reasons.

13. A real-time vehicle or equipment management system according to claim 1, wherein said real-time vehicle recording system is substantially stored in a stop and control box to prevent unauthorized access thereto and the vehicle.

14. A real-time vehicle or equipment management system according to claim 1, further comprising a payment mechanism in or on the vehicle, responsively connectable to said at least one processor, said payment mechanism collecting vehicle information and providing real-time billing, debiting or crediting from the vehicle, and retrieving at least one of a script or electronic signature from a card carrier, and verifying the identity of the card carrier via at least one of photograph, fingerprints, and identification.

15. A real-time vehicle or equipment management system according to claim 1, wherein said at least one processor performs at least one of the following functions:

remotely controlling at least one of robotic functions to activate and control vehicle operations, remotely billing for use of the vehicle, remotely operating at least one machine, evaluating and diagnosing computer or processor malfunctions, remotely ordering materials and service personnel to perform at least one of service and repairs, remotely performing price quotes for cost of the at least one of service and repairs, remotely performing repairs electronically, and remotely shutting down equipment;

remotely controlling data exchange representing a monetary exchange via a focal node to perform a secure and protected containment function of: to restrict unauthorized use of equipment, to record and preserve data in an acceptable legal manner, and to bill at least the vehicle user, thereby providing a total accountability system;

at least one of networking and communicating with at least one gateway to other computers and computer networks that manage data, said gateway determining whether the other computers and computer networks are to be at least one of networked and communicated with to further monitor and store data for at least one of billing, regulatory compliance and legal compliance, and optionally for at least one of social economic and environmental impact;

at least one of networking and communicating with at least one of other computers and computer networks that manage data, including at least one of vehicle location, equipment technical assistance, personal accounting for machine or equipment use, billing, debiting, crediting, vehicle operations, service and repairs; and

monitoring equipment for health and safety conditions potentially adversely affecting the public, including at least one of reckless driving, driver impairment, pollution, vehicle unsafety.

16. A real-time vehicle or equipment management system according to claim 1, wherein said at least one processor performs at least one of the following functions:

collecting machine message data from said real-time vehicle recording system used to compile data for a public media or web page, and transmitting the machine data thereto;

presenting the machine message data on at least one web page that originated from at least one equipment on said real-time vehicle or from a machine messaging network;

recording and reporting to a monitoring gateway for billing for highway use by the vehicle;

collecting and storing data corresponding to charging at least one electric vehicle;

reporting, recording and billing automatically using a real-time billing system in the vehicle corresponding to time a geographic area roadway is used;

determining impact on environment including roadways, using at least one sensor recording at least one of:

weight and emissions ratings for atmospheric impact type of at least one of fuel and energy used;

time of operational machine use;

amount of fuel or energy used;

type of waste product produced; and

amount of the waste product produced.

17. A real-time vehicle or equipment management system according to claim 1, wherein said at least one processor performs at least one of the following functions:

recording at least one of audio and video traffic vehicle impact, and recording and reporting to at least one remote monitoring system for at least one accident investigation and machine accidents in a data secure manner;

recording information used in insurance investigations to decide claims and assign liability;

determining liability and accountability to be used in legal proceedings and optionally to be used in determining safety parameters, rules, regulations and laws;

recording at least one of audio and video captured criminal incidents by activating unattended vehicle systems to report criminal events through remote control;

recording at least one of audio and video captured news events as witnessed by a machine system including at least one of weather conditions, and traffic conditions.

18. A real-time vehicle or equipment management system according to claim 1, further comprising at least one operations sensor recording information including at least one of operations of the vehicle, highway conditions, speed limits, driving conditions including speeding, reckless driving, drunken driving, road rage, pensive or inefficient driving, and wherein the information of the vehicle are received from said operation sensor and stored in said memory and downloaded to at least one of a remote monitoring system, a remote billing system, and a remote data analysis system.

19. A real-time vehicle or equipment management system according to claim 1, wherein storage of the information includes storage with two onboard and at least one offboard storage of the host piece of equipment, the offboard storage optionally including application specific Email or warning flag detailing an electronic serial number associated with a privately owned or personal E-mail address.

20. A real-time vehicle or equipment management system according to claim 1, wherein the PFN includes more than one purpose optionally billing for commercial service or for specific service of a machine and simultaneously gathering data on any incident or accident event or provide additional controls by off board control and/or management systems in an emergency or in the case of a compromised operator in real-time.

SECURE ACCOUNTABLE, MODULAR AND PROGRAMMABLE SOFTWARE "TRAC" FOR PFNs, PROCESSORS, CONTROLLERS, AND COMPUTER NETWORKS TO MONITOR, MANAGE, STORE AND REMOTELY CONTROL DATA AND EQUIPMENT

RELATED APPLICATIONS

This patent application claims priority from U.S. Provisional Patent Application No. 60/---,---, filed May 1, 2000 (110273-700); U.S. Provisional Patent Application No. 60/176,818, filed January 19, 2000 (110273-401); and U.S. Provisional Patent Application No. 60/139,759, filed June 15, 1999 (110273-500), all incorporated herein by reference.

This application is related to U.S. Provisional Patent Application Nos. 60/122,108, filed February 26, 1999 (110273-400); 60/071,392, filed January 15, 1998 (110273-201); 60/089,783, filed June18, 1998 (110273-300); 60/032,217, filed December 2, 1996 (110273-101); PCT International Patent Application No. PCT/US99/00919, filed January 15,1999 (110273.202); U.S. Patent Application No. 08/975,140, filed November 20, 1997 (110273-100); and PCT International Application No. PCT/US 97/21516, filed November 24, 1997 (110273-100) all of which are hereby incorporated by reference.

BACKGROUND OF THE INVENTION

Field of the Invention

In the related patent applications, the PFN is described as a hardware device that is called a protected primary focal node that ultimately can be placed almost everywhere or on anyone to perform accountable remote monitoring and control including for vehicles, machines, and equipment. With further development including tracking, physical telemetry and remote control use for personal PFNS to help manage and control provisionally free individuals and or animals by the appropriate protocols and authorization. Basically all PFNS are designed to monitor accountably from a secure environment, and provide aggressive remote control capability to equipment and people in any physical environment. There are even application specific PFNS to operate independently report on and perform remote control activities in the environment. PFNS will include any and all actions of machines and or man for the purpose to acquire specific data on conditions perform activities or functions; and to record this data on location, as well as, report it back redundantly to any appropriate

concerned individuals, and or the public in general through wireless and wired communications via computer networks and made accountable through data storage systems. This can be a closed circuit monitoring and remote control systems, and or one that is networked either publicly or privately on a larger scale. It may utilize or include in many cases the World Wide Web for inexpensive mass access and handling of data, which can be provided with medium to relatively high commercial security protocols through this technology's software innovations and Commercial Off The Shelf C.O.T.S. products. Running in any PFN/TRAC System.

The PFN/TRAC system is designed to couple with existing technologies and provide protection and accountability and to augment any system with a full array of tracking products, audio, video and varied sensing devices as well as activity controls and innovative actuators to perform many task remotely.

So this patent will utilize existing C.O.T.S software products (widows based programs, etc.) that are available today and are easily configured for the purposes, stated throughout all the related patent applications. Many interfacing applications will employ marcos (application specific) to combine to running software programs through automatically activating hardware functions, e.g., (Key strokes) to create a new software response as part of 1000 series control "coyote trickster" interfacing of existing C.O.T.S. products that are incapable of software augmentations directly. It will also, however, offer proprietary configurations for new uses of any C.O.T.S. software products as well as, provide a unique modality to handle data in an accountable manner in the PFN and TRAC system. Or for the use of TRAC with any other processor that require accountability for activity controls and or sensor inputs. TRAC stands for Trusted Remote Activity Controller and is the programmable and modular software necessary to provide accountability to aggressive remote control for society and it's institutions. The objective of this technology is to provide a secure communication and data management system initially in the PFN (the protected primary focal node) with TRAC a most unique and ideal software modality, that can be used as a universal program and or a standard, to format accountability for aggressive remote control. The technology will seek endorsement by the insurance industry to provide trusted accountability in the liability assessments and rate assignments for aggressive automated and remote control in any scenarios. Automobiles and highway travel and safety will be a major focus of course, but this technology is planned to provide this secured trusted analytical data tool for every insurable area and every purpose on earth. The total goal of this application is to also receive approval and certification from the Banking Industry, Government agencies, Security organizations, the Automobile Industry, the International Electrical Engineers association,

computer engineers and or programmers associations, and or any other Science, Technology and Society concerned citizen groups, organization, and or commercial interests.

The TRAC system and software will be programmable and modular and deployed as software and firmware in all types of hardware configurations (application specific choice determined by engineering for product purpose, practicality or cost effectiveness). It will also employ analog and digital signals and data streams including; audio and video technology as well as telemetry for man and machine operation and the environment along with any other application specific data streams determined as necessary or is the main reason or purpose for any PFN/TRAC deployment.

This application is providing this TRAC firmware and or software system so that it can track any electrical signal received and or processed by the PFN/TRAC devices as well as, track and record any application specific reactions to those signals by any host equipment, personnel, environmental condition or change; and also, continue the accountability functions for off board tracking, through the management and storage of data handled through the PFN/TRAC monitoring and or remote control system and or Network.

The remote control accountable software for tracking will require personnel Identification, electronic serial numbers ESNS, from the transmission equipment used, GPS, and stationary systems may use land line numbers and coordinated addresses, etc., and or any other locating systems data to be converted from a data signal at the application level in the end user computer to place an object on a calibrated map as latitude and longitude coordinates. There will be time and date data as well for every command and application specific reaction performed by the host machine via a PFN, or due to any remote control commands which are simultaneously stored in a local memory and redundantly transmitted transparent by wire or wireless with Internet Protocols to be available as text, graphs, spreadsheets, photos, audio or video, etc., at the application level when required for review or analysis either in real-time or at any later date. This is to be standard operational data acquisition necessary to perform any credible remote and or automated function completed with a PFN/TRAC system attached. Application specific PFN/TRAC systems may use all these data streams or just a few select one. Basically the TRAC system in the PFN is a modular and programmable system that will authorize and authenticate commands and activities for aggressive automated and remote control with local and remote redundant memory systems. This is how this technology plans to provide a trusted remote activity controller to provide accountability to obtain approval from the public, insurance, industry and government. The manufactured commercial products employing this technology's PFN and or TRAC systems will be responsible for obtaining any and all certification proof testing in their design, construction and applied use, as well as,

indemnify the inventor and the primary assignees Kline Walker LLC for any damages or liability in any exploitation of this technology and it's related innovations. The PFN/TRAC System is designed to win approval in industry and government standard efforts for performing accountable remote and automated control. The technology is also designed to incorporate all other automated control and communication technologies in this process to form a well organized web of local protected accountable interface platforms that can create a machine messaging set of networks (integrated as needed) on a global scale to better manage man and machine along with the world environment. The goal in developing the PFN/TRAC system is to provide a real-time data acquisition and management system to promote trust and cooperation in the world's populous for the sensible use of technology and resource by managing the negative impacts on society, economy and the environment thereby sustaining humanity with more freedom, responsibility, fair play, safety, and improved health for the best personal pursuit of happiness in all societies.

Specific Accountability Functions

The mass of all data collected in real time for first level temporary memory shall be controlled by being erased in a re-writable memory and not stored in the permanent memories (local) if deemed unessential by application specific onboard firmware and/or software criterion, and not reported redundantly to any remote location unless countermanded by the off board monitoring and control systems, e.g., TRAC/FACT FTP, CEW etc. defined in the body of the text).

This technology has provided for it's PFNs and or any other technology's processors or programmable controllers a set of secure accountable software comprised of programs and designed to be modular. The base and or operational system once again is termed and referred too hence forth as TRAC, which stands for Trusted Remote Activity Controller. This is a programmable modular system in the PFN that authorizes automated and remote activities and then authenticates the response and store the data in a plurality of memories. The specific protocols ideally to be determined by standards committees, to structure the application specific guidelines for this technology's deployment to safely and appropriately full fill society's needs and requirements for aggressive and or passive remote control and robotics. Finally the PFN/TRAC Systems will have numerous fail safe or backups systems but ultimately the TRAC programming will be able recognize and mark when it is malfunctioning and not providing accurate and accountable records. This is a major purpose and function of the Trusted Remote Activity Controller.

Brief Description of Drawings

Figure A1 is a cover sheet for the PFN/TRAC system showing the four main areas of involvement; Control Security Technology, Mobile Management, Home Management, and Commercial Management.

Figure 1 is displaying the Trusted Remote Activity Controller TRAC and describing the software protocol to create the accountable system for remote control and management.

Figure 2 is a more in-depth breakout and description of the many application specific programs that will run in the PFN/TRAC System either in universal diverse PFNS or application specific PFNS.

Figure 3 shows the two basic different communication PFNS which are one way communication systems with only local real-time event memory storage for accountability and two way systems that provide a redundant remote memory storage.

Figure 3A is a continuation of the one and two way PFNS and is a chart that details the properties and qualities of the communication devices used in the PFNS.

Figure 4 details the physical architecture and hardware components of one way communication PFNS that will run the later detailed software programs of TRAC.

Figure 5 details the least expensive two way communication PFN system (two way paging) hardware component architecture for the PFN/TRAC System.

Figure 6 is the most sophisticated of the PFNS and it is the two way RF or Cellular or wireless telephony communication system capable of carrying real-time video to a remote location as a major attribute. This drawing is of the hardware component architecture utilized to construct these PFNS and TRAC system.

Figure 6A is a Figure showing the progressive evolution of the PFN/TRAC hardware architecture designed into the PFN/TRAC system to keep it current as a future technology.

Figures 7 and 7A are but some of a group of similar drawings that appear through out all the PFN/TRAC applications showing the classic double wall physical structure of the encasement that protects the PFN/TRAC node. The architecture in the same but the materials and configuration changes per application specific structures are going to be part of a standards effort even though the PFN/TRAC systems have addressed and created certain configurations for certain applications. (Note PFNS can be secluded or protected or both and protected differently than this set of configurations.)

Figure 8 was of one of the first add-on PFNS for credit card billing and charging in real time for cabs and mobile applications, it is an earlier version of the PFN stop and control box but is shown in this application as a unit that would run TRAC software programs and use Financial Transaction Products as detailed in the TRAC system software.

Figure 9 is a first drawing of a one way pager encasement to protect the interface and memory for the original stop and control box. The two way pagers can be housed in tight of a configuration as well with different programming

Figure 10 is a illustration of a PFN encasement in the dash of an automobile with connectable interfacing on a pager systems and cellular phones as well as a interfaced lap top.

Figure 11 shows the adjustable compartments and structure in side the car dash PFN.

Figure 12 is a 3 draw configuration for the car dash PFN hard ware detailing the possible components essential n the PFN and also the personally owned electronics array of personal items that can be interfaced.

Figure 13 is a diagram showing the different communication devices in the PFN and the card swipe magnetic reader for financial transactions, it also shows the three major types of wireless servers or providers for communications with the PFN/TRAC system, paging, wireless telephones and RF systems

Figure 13a is an enhancement of a earlier drawing for the universal PFN and it incorporates technology from 6a showing the unibus and some more consolidation of devices and systems.

Figure 14 is a drawing that details an electrical sealing system used to certify at least the event memory storage area in a PFN/TRAC system as untouched and that the one write memory is still in a pristine record state for evidence grade use.

Figure 15 is a hypothetical PFN encasement showing the state seal system and it's anchors in addition to the physical locking mechanism used to protect this area.

Figure 16 is a federal agency directory that supports web sites and has and will provide numerous gateways on to the Internet as well as to other isolated agency intranets and will be part of PFN/TRACS Federal Access and Control Technology FACT.

Figure 17 is a diagram showing many PFN/TRAC applications around the world and how it serves the public within formative web pages, the government structure for taxing and aid and the economy with commerce as well as the world environment as part of a gigantic machine messaging net work for monitoring, managing and controlling equipment and that equipment's impact. Not shown here are the personal PFN products.

Figure 18 is the Federal Access and Control Technology FACT called a chip here but can basically be in the form of any kind of hardware, software or firmware, and has as a main purpose to provide identification of a component and make accountable the component and user in the PFN/TRAC/FACT system and control that component in real-time by a series connectable registries from local to national and globally if so desired.

Figure 18A is a Figure of the PFNTRAC system running Federal access and control

technology FACT programming.

Figure 18B details the government FACT registry down to the responsive component level.

Figure 19 shows the registries and wired wireless and IP links in an acceptable present day configuration as to the state of world affairs and trust. An area that hopefully can change and be more open with all nations.

Figure 20 shows how the FACT system software will accomplish new installs and reinstalls of components in to the entire system individually at each local PFN/TRAC node.

Figure 21 details a software flow chart on how FACT will be allowed to access individually owned PFN/TRAC systems openly and sets the parameters and guide lines for stealth access. As perceived by the author with respect to the constitutional right and respect for individual privacy. (This is only conceptual to explain the functions) public and government will set policy and laws then programming protocols will be set and application specific software will be written.)

Figure 22 is detailing the alert status of a component entered into the system that may be flagged due to national security, part recall, or theft etc. This diagram discusses how the software flow could go in some of these scenarios but once again this will be laws, standards and regulations all before the software commands are entered into and application specific hardware configuration

Figure 23 shows an earlier patent drawing for the personal PFNS and it is a universal application PFN showing various communication systems. In reality may be only one com link will be used to save space

Figure 23A is one of the personal PFNS using the Radio Frequency system of a walkie talkie.

Figure 23B is another communication modality for the personal PFN using 2 way paging protocols.

Figure 23B1 is an earlier Figure using reflex 2 way paging protocols to create personal tracking and PFNS.

Figure 23C is a cellular modality to transmit data for the personal PFN.

Figure 23D incorporates a predicted communication development by the PFN technology and is a usable asset in the PFN/TRAC system.

Figure 23E is the total configuration belt for many activities and different communication possibilities and uplinks. It is in no way all the modalities and uses of a personal tracking system or accountable PFN; but it is a good representation of the inventions possibilities.

Figure 24 is a diagram exploring many of the personal PFN systems and tracking devices.

Figure 25 is showing some of the most immediate equipment uses and areas.

Summary of the Invention

Present PFN Technology Defined.

The nucleus of Kline and Walker technology is a protected control component called a Primary Focal Node. A Primary Focal Node (PFN) combines wired or wireless communications, processors, activity controls, sensors, audio and video telemetry in a physical, electrical, and legally protected interface platform constructed to provide accountable remote control and management through local and remote redundant memory storage. There are two basic Primary Focal Nodes (PFNS) that have been designed to help address Industry and social standards by providing Accountable remote control and management for equipment and life assets e.g., (people and pets, etc.).

Security is provided through physical and electrical means. And Accountability is accomplished by secure local event memory storage and redundant remote memory storage to at least one remote location.

The PFN is designed to be a Trusted Remote Activity Controller TRAC termed by the technology as a PFN/TRAC System.

Along with the PFN hardware control interface component the PFN/TRAC System has operational software and firmware termed TRACS. TRACS is the base operating system name for the software programs running in the PFN computers or processors, including any connected remote monitoring, control or management systems, either for general PFN software applications or any application specific configurations.

This software and it's functions are the main focus of this patent application. The PFN/TRAC System or device can perform as a primary activity control interface with individual human beings or animals or be a control interface on a piece of equipment as part of a remote control intranet web or be part of a much larger system like the Internet or the World Wide Web.

Base Function of a PFN

PFNS can act as repeating stations (either preprogrammed digitpeating or repeat analog signals) with other PFNS or other communication devices to create a flexible mobile and stationary web through preprogrammed protocols, that scan convert and route electrical signals from various wireless messaging devices and systems, to summon emergency

services, interface with the Internet or perform application specific network tasks or activate any electrically controlled local activity in an accountable manner.

PFN modalities promote EASY PFN COMPONENT INTERFACING: A standards effort will be at the forefront of any commercialization and an on going process to establish the universal PFNS as well as Application Specific Configurations to minimize interfacing problems and maximize versatility in wireless machine messaging.

A basic quality of the PFN interface is to provide user friendly PLUG, PROGRAM, AND PLAY simplicity for the end user, with interactive controls, while addressing as much as practical forward and backward engineering possibilities to create a rapid commercialization of this accountable organizational component for machine messaging and wireless personal management scenarios, e.g.,using a machine messaging network in conjunction with the World Wide Web (MMNWWW)

The PFN technology additionally includes Commercial Off The Shelf Products and C.O.T.S. interfaces to promote versatility and capability through the PFNS for quick accountable control and management scenarios in existing machinery and for updating and converting existing equipment and systems for other remote control scenarios. As part of Kline and Walker PFN/TRACK technology's nature and scope of invention, the consolidation and integration of circuit architecture for all components and accessories is specified in all the related patent application specifications to provide longevity in the market place and is considered an important and valuable asset to providing space and versatility for interfacing other technologies.

PFN Communication Mediums Include:

Radio Frequencies, and repeating or digitpeating technology and protocols. Pager Frequencies and protocols with accompanying Commercial software and hardware Systems, Cellular Phone Frequencies with wireless phone protocols, software and hardware considerations and accompanying Commercial Systems for Satellite or RF, or wireless telephony, and TV, both commercial and governmental, all bands including L Band (military), Cable TV, IP protocols, land line (telephone ISDN, fiber optic and all data routing systems), as well as Internet providers and servers.

PFN/TRAC INTERFACE COMPONENTS INCLUDE:

Sensors, transducers, mini computers, processors, memory storage, universal pug and play unibus system, activity controls, actuators, GPS and locating technologies, audio and video, personal identification systems, voice recognition technology, displays, communication terminal devices (keypad, etc.), wireless communications transceivers/devices

and connectable remote communication systems, physically protected enclosures and electrically protected hardware system, tamper resistant and detection, software programming, current and signal sensing circuits and devices, independent power source, solar cell and chemical and electrical energizing systems, transformers, power regulating systems and discretes.

PFN APPLICATIONS INCLUDE:

Personal PFN application specific uses include (e.g., first products offerings and markets). Personal tracking and telemetry products in the form of belts bracelets collars, article of clothing, personal items purses, brief cases, mobile offices, multi tasking communication and personal computers, organizers, palm tops or locating products, physical implants, with remote control applications for nursing and policing. Health care telemetry with prescribed remote treatment and patient management, child monitor or care and protection, e.g., school link, camp view, ski seeker, passenger pointer to locate crash victims, boat, plain train and auto, the conditionally free for parolee guidance, management and control–victim protection and peace of mind, Animal Shepherding, Pet and animal location management and or controlled, farming, live stock telemetry, or Crowd control policing-guidance and management directional aids, or marshal law, incarceration scenario, head count, identity checks, public safety and accountable aggressive security controls nation building with peace keeper function to be coordinated with Equipment PFNS which are accountable machine messaging net work nodes.

Equipment PFN applications include (not a complete description of PFN products or involvement):

Environmental sensing and monitoring for local and global impact to determine policy and change, as well as determine, availability, quantity, cost, profit, tax, or penalties for good management of resources, and energy, with more of the same for all commercial and private machine use, including remote operation, and automated repair or diagnosis, augmentation of accessories in; agriculture, e.g., tractors and farm machinery, construction, earth movers, etc., industry/manufacturing, e.g., production or material handling equipment, and transportation/vehicles e.g., smart car systems and interactive highways, cars, trucks, buses, or rail systems trains, trams or on the water, boats/ships and aviation as well to perform auto-tutor and emergency control and management functions during human operational learning curve periods, to automate military equipment, nation building, national security uses, governmental assessment of equipment use for tax to support society's infra-structure,

highways, bridges, etc., private and home use for combined utility, security, public safety and energy use as well as impact values on environment and community infrastructures to provide automated or remote management and control, also to analyze in real-time the commercial value, cost and loss for financial investments e.g., companies and technology on the stock market. Bank loans, insurance risks. Many more of the specific inventions PFN innovations, separate but related inventions, applications and uses are detailed in the Kline Walker patents and any disclosure is forbidden with out authorization.

This application details the accountable modular and programmable software termed TRACS that authorizes and authenticates commands from wireless and land line telephone and or RF equipment and or light transmission technologies to remotely activate and confirm automated controls and functions through processors controllers and or computers. As TRACS processes this data in a secure manner it stores it in a protected storage on board a piece of equipment in this technology's PFN on location and in the case of the two way transmission PFNS it reports it back to at least one remote location for a redundant memory storage.

The PFN/TRAC system was designed to distribute communicated commands to their appropriate application specific preprogrammed protocols while authenticating the authorizations and preserving and accountable record on both sides of the remote control communication and through out any redundant transmissions or data storage that is interfaced and networked. The TRAC system of software has been designed to develop a Trusted Remote Activity Controller for all of societies needs regarding accountability and liability as well as to preserve an organize secure modalities to mange and control automated equipment, and financial legal transactions.

With the advance in electronics, communications and computer processors the automation of equipment is rapidly approaching aggressive remote control and robotics and needs to be made as accountable as the owners and operators have been solely responsible for in the past. Because, control responsibility will be shared at first between man and machine and might very well always be this way; accurate telemetry of both will be essential to provide organization and proper management and legal control in this scenario. This technology's PFN protected primary focal node and The TRAC software system has been constructed to provide the means to accomplish these control and accountability tasks and to serve as an electrical interface, physical platform, and software control center to write standards and software programming and protocols.

In conclusion the PFN/TRAC invention's base objective which has been stated redundantly though out the PFN applications is to incorporate present, past, and future

modalities by providing flexibility in constructing PFNS out of existing technologies and to establish an organizational platform to perform accountable local interfacing. The progressive consolidation of these devices, components modalities are well documented in PFN applications and all fall within the nature and scope of the invention.They are meant to be inclusive in the specifications and in the claims of the PFN invention and to deter proprietary development. This was done deliberately to draw all manufactures into a cooperative effort to organize and standardize an accountable interface platform and system for accountable machine messaging robotics and remote control and management. This needs to be done as an industry standard; So basically these variations and modalities are also offered to aid anyone skilled in the arts to have all the options and versatility to interface there devices and product within the PFN/TRAC System. It is a major objective of the PFN/ technology to be an inclusive, not exclusive and to perpetuate equitable sharing of knowledge data and cooperation to increase markets, products and services for the public and the economy. In no way is this deliberate attempt to negatively stave proprietary development meant to restrict any new developments or improvements, nor is this invention designed or developed for such a purpose, as is stated by the inventor Richard C Walker. The opposite is the case and intent. A cooperative effort to develop any new and improved diverse but more universal technology that enhances PFN/TRAC System and accountability as an improved evolved organizational interface for remote control and robotics will always be encouraged and given access to any market and PFN/TRAC System in use as long as I can personally can influence this process.

Detailed Description of Drawings

Figure A1 is a Overlay Sheet for PFN/TRAC Technology PFN/TRAC Remote Management Systems. This is not a Figure as much as it is a cover sheet for the technical Figures. It shows however all the areas of control and management that the PFN/TAC system is designed to be a part of and integrated into. The PFN/TRAC System is at the center of four basic areas involving machine messaging. It is there in two ways, first locally in the form of a physically protected remote control interface platform with accountable memory and second as shown here intrinsically as a center for control and management of these four areas. Which uses the PFN/TRAC System of networks to monitor and perform individual or mass control or management functions through a Machine Messaging Network both separate and connected to the World Wide Web or Internet. Part of the PFN/ TRAC System is a nationally operated Registry termed the Federal Access and Control Technology FACT that is explained in greater detain in this application but provides all governing agencies their own special

communication ID's and access in all four areas, but with special protocols to protect and respect individual privacy protect and serve the individual and the public while providing controls for any "big brother abuse" ref. books (1984 & Brave new world). The same is true for commercial interest, organizations as for individuals. The use, development and deployment of PFN/TRAC devices and any monitoring and management system has deliberately been designed in the spirit and scope of a complete real time democracy. The design is also structured to be developed through the United State constitutional guidelines and guarantees as provided by the bill of rights to the individual citizen, while providing an organizational structure for the merging technologies of communication, computers remote control and robotics in data acquisition. It is also designed to coordinate and organize agency services and responses to increase public safety and national security.

The system has been designed to help control, criminal activities and manage the use of equipment, while appraising environmental and infrastructure impact as well as provide individual assistance and services to those in need. (Application specific for personal PFN/TRAC devices and Equipment PFN/TRAC devices). Both personal PFNS and Equipment PFNS are used in all the same areas and also utilize much of the same components and communication systems, but are provide different arrays of sensors, activity controls and actuators.

The top left ball for control security, is remote control and management with the highest security functions for private, commercial, and governmental applications and is covered extensively in the earlier related applications. This area would have a great deal of local FACT registry contact in the commercial, and individual applications and the DOD and national security agencies would have their respective involvement as well as the military in their application specific areas. The right top ball is for home management and will be responsible for home security, utility use, remote equipment repair diagnosis, supporting a local repeating center and beacon (application specific for all PFNS), home security, interactive with wire and wireless appliances, family safety, sense fire or panic situations and contact the correct assist personnel, etc.

The lower left Mobile Management is for all moving platforms personal, private, commercial, agricultural, etc. to report on activities, resources use and impact on environment. And finally commercial management of stationary equipment or material handling equipment in factories, and large installations, which report on many pieces of equipment for both in house isolated intranets and with an IP FACT or Internet connection to other intranet locations or on the Internet and government nodes.

Figure 1

Trusted Remote Activity Controller (TRAC)

OPERATION

The Trusted Remote Activity Controller provides all local vehicle or device control and event storage relative to PFN (Primary Focal Node) operation. It interfaces to an RF telemetry link, which may consist of a one or two way paging system. More sophisticated links could be used such as digital cellular or PCS (Personal Communication System). Typically, a Remote Management System (which may be as simple as a single page, or as complex as a controlling PC or Server) initiates a TRAC function, such as an automated slow, stop and secure sequence. The signal or paging command is received securely (via encryption) and decoded by the TRAC. Optionally, a local display or audio speaker may provide local status of the TRAC function being executed, with appropriate progress tones, voice queues or displays to provide a local operator feedback relative to the progress of the function. In performing the function, all activity controls are initiated by the TRAC and monitored by the TRAC from start to finish. This is accomplished through feedback sensors. Feedback Sensors may be electrical, mechanical, fiber optic, infra red or other technologies. Since the function being performed requires a high level of accountability and trust that the sequence was in fact executed properly, every step of the process is monitored through appropriate feedback sensors to attain the reliability and trust required. This positive feedback in the TRAC is the key feature which distinguishes the TRAC from other electronic or software controllers; making it a fully "trusted" system for the task being accomplished. Additionally, all events and status relative to the function are recorded locally in the Local Event Storage Memory. This is termed the System Function Data. The level of redundancy in storage of System Function Data and the level of additional feedback and checking required in order to verify the activity or function was accomplished properly, is directly related to verification requirements. These requirements may be regulated and approved by local or federal law, law enforcement or insurance agencies, World Bank, EPA, ICC, SEC or other regulatory agencies.

Interim progress of the sequence, activity or function may be optionally transmitted back to the remote management system through a 2-way phone or paging link. This may occur as the function is executing or may be programmed to occur after completion of the sequence. In any event, local, redundant storage of the event is always contained within the PFN for subsequent or simultaneous retrieval of event information and proof for accountability purposes. The PFN enclosure and TRAC monitoring of tamper sensors guarantee the information has not been compromised. Other types of information along with

the System Function Data may be stored in the TRAC Local Event Storage Memory. This auxiliary information may include digital or analog data not directly related to the function being monitored and executed, but important for evaluation and determination of liability, collection of evidence or environmental data. Examples of these include road condition information or surveillance audio and/or video.

IMPLEMENTATION

TRAC implementation may be accomplished in many ways, depending on space or funding constraints and level of integration required for the system. A PC-based system may be in the form of a desktop system, laptop, palmtop or embedded system (PC 104) with a dedicated DOS or Windows based TRAC program, consisting of machine language, Basic, C, C++, Visual Basic, Visual C or C++, or other high level language which accomplishes the TRAC function through software control. Interfaces to the System Under Control (SUC) may be accomplished through appropriate I/O cards, either analog or digital. PC compatible Modems or Cell phone interfaces provide the interface to the Remote Management System (RMS). SUC and RMS interfaces may be in the form of ISA, PCI, PCMCIA, VME, Compact PCI, Future Buss, or other commercial interfaces compatible with the PC-based system used. More compact and custom implementations of the TRAC may consist of dedicated state machine controller implementations in which TRAC functions are executed through embedded firmware. These implementations may incorporate multi-chip solutions using EPROM or EEPROM interfaced to Arithmetic Logic Units (ALU), I/O ports and discrete memory elements. They may also be microprocessor or microcomputer based. A large variety of board level products are commercially available for such an implementation. Single chip or high density implementations might consist of Field Programmable Gate Array (FPGA) or Application Specific Integrated Circuit (ASIC) based devices. These implementations may incorporate all sequencer, firmware, I/O and storage functions on a single device and would provide the highest level of integration and smallest size. Display, Video and Audio (Auxiliary Data) for the TRAC can be in many forms and types. These may range from analog systems, in which tape or other magnetic media store the analog signal, to digital systems in which data is stored on hard disks, EEPROM or RAM. Data format may be modulated through FM or AM, compressed, packetized or otherwise encoded for reduced bandwidth or for transmission over the Internet (packet audio and video).

The vast amount of possibilities and form for the TRAC are deliberately designed into the PFN accountable organizational interface and is a continuing effort to be as inclusive as possible of all technologies to provide versatility and universality for the public and the free market.

Figure 2

This second Figure of TRAC is a more detailed description of this technology's proprietary programs interfaced in the programmable and modular TRAC, for mobile management, commercial management, home management and the control security technology applications detailed throughout the related patent applications. In this drawing the cube labeled TRAC displays all these Application Specific Software programs (ASS). This software is programmable and modular. The TRAC software can be in the form of hardware with embedded software or firmware, or it can be modular software running in processors controllers and or computers (these applications and product directions will be determined by engineering preference at the time of manufacture or any current owner of a PFN as applicable by how flexible the PFN architecture is.

The Software/Algorithms will accommodate Bank and stock exchange Transaction products, which will be supported by this technology's FTP Financial Transaction Program (C.O.T.S. or Proprietary). This program will do as much as possible to support run and route any C.O.T.S. products best suited to the owner of the host equipment and their choice of commercial servers, but eventually all programs will meet certain securities exchange and banking standards. This technology plans to utilize Commercial:128/64 bit Encryption for Web Transactions with the present proprietary software program to support and interface most of the secure commercial exchange products with all the pretty good protection PGP software C.O.T.S. products available today. This Program is labeled Commercial Encrypted for the Web (CEW). These transactions might be used for service billing for privately managed credit card account service companies etc., dealing with a specific clientele and their equipment. This system could provide inexpensive direct billing to personal and company E-mail addresses, rather than going through a large bank card programs with all their expensive costs. And or the bank card companies could utilize the financial transaction products FTP product constructed to provide the adequate security protocols for a secure track able transaction record including identification for equipment and personnel, as well as, time date and location of any transaction. (Finger prints and papillary recognition hardware cameras and sensors, etc. would be employed along with the accompanying software algorithms to document and authorize as well as, authenticate any transaction. However, initially the key pad or any interfaced phone number pad will be utilized to provide personal identification numbers PIN numbers for the transactions). However, specific protocols and software programming will be determined by industry standards.

FACT is the federally authorized control technology or access and control technology protocol and or standard. This program will take priority over all running programs on any

PFN equipped piece of machinery equipment and or vehicle. It will be used by law enforcement and authorized government agencies for national security and public management and or crowd control in extreme cases such as, a declared state of marshal law. It will be a priority system over all host equipment functions including financial transactions to insure fair and stable pricing in providing necessities in a ravaged and or compromised area. The financial record can be reviewed later to determine any improprieties exploitation's, and or profiteering that occurred and is so prevalent in these kinds of circumstances, where black markets and improprieties create a lack of trust and disharmony between warring factions. These are nation building functions and extreme Control Security Technology applications.

FACT will also be responsive to special reserved RF radio signals for police and official government access as well as be responsive to specific coded and encrypted messages sent and received on any frequencies including digital and analog signals and ID protocols (specific address Electronic Serial Numbers, ESN, etc. This is to allow immediate individual, identification communication and control of a vehicle it's PFN interface including all equipment or components as well as any host equipment electrical system and the same level of control for all area PFN vehicles and equipment in an emergency. A standards committee will address the specific protocols for the utilization of this function and law, rules and regulations will spell out the guidelines as is legislated and approved by the public. Another base function of the FACT is to perform integrity checks of PFN components interfaced to make sure they are licensed products that are interfaced are not reported stolen products or that the PFN is not attached to a stolen host product through a special FACT chip or embedded program in each component/device. This is accomplished as a review process performed by the FACT registry that is detailed in Figures 18, 19, 20, 21, and 22. Each time the PFN installs a new component (performed locally by fact embedded firmware program), which is part of a manufacture FACT registry responsibility. This variable use value tax structure provides revenue for states or regional governing bodies for a new component is used in their location, as well as resale products with no inconvenience to any individual seller. This should prove more profitable and accurate than collecting sales tax only on new product sales either on the Internet or in area stores freeing up both for communication and commerce. PFNS provide a mechanism for real-time use taxing and real-time impact and assessment on societies infrastructure and their environment.

The local PFN/TRAC system is in a secure encasement with local memory and remote redundant memory and designed to perform at a triage level providing; accountability and analysis of any event as well as make it easier and more instructive to use PFN equipped

machinery or PFN assisted personal activities or monitoring in the future. FACT program will be accessible by the police, law enforcement, and or traffic enforcement system and police remote control command tools, that are capable of locally identifying a vehicle and controlling a shut down of that vehicle in the manner well detailed in earlier related PFN and Stop and Control Box applications for this technology's proprietary "spider eyes program" or for any smart car and or interactive highway programs. Of course law has to be legislated and rules and regulations made and well understood as to the manner of engagement and the procedures to use these devices and systems to preserve respect for the legal rights of the individual as public safety is being served and provided. The laws are clear and exist today. Only the rules governing the use of this technology have to reflect the true intent of the law and the PFN can provide an accountable record to make sure the all follow the law or are liable criminally or civilly for their actions or improprieties regarding any misuse of this technology. (Everyone has a record of the event and all constitutional law applies to the use of that data.) With this in mind the actual software commands will be dictated by the legal rules regulations and law that will determine the programs activities. So the software architecture presented here is in the form of flow charts till society and their government agencies address their specific responsibilities and the rights of the individual for these program parameters. Also, the specific software architecture and hard ware components will be determined by government and industry standards and preferential engineering concerns. However, this invention develops numerous modalities to accomplish the construction of local PFNS and how to construct the monitoring and management system in varying levels and degrees to provide product for all commercial venues, so that anyone skilled in the respective arts of electronics, communications and computers given enough man hours can build the PFN/TRAC device and system for any level. For that reason any variation in construction of an accountable electrical interface system providing monitoring and remote management and control to or for man and equipment, fall within the nature and scope of this invention.

FACT will also, provide varying degrees of security protocols all the way up to and including DES data encrypted standard at certain levels for any and all equipment if so determined necessary in the legislative process or in a special uses format for national security or military applications around the world. This technology provides for the use of broad governmental management and control through a modular modality to be deployed physically in chips and or activated as pre programmed software/firmware in any PFN processor or PFN interfaced processor, for special situations as authorized and agreed upon by the appropriate governing bodies for domestic civil situations and or world peace treaties to insure fair

treatment and management in these hostile situations, where terms of an agreement or contract have to have some form or mechanism to provide mutual fairness (where TRUST among parties is deficient).

Federal Access Control Technology (FACT) has been designed to be set up and governed by the United States democratic process as a master control standard for this technology's machine messaging network and to include the world wide web to comprise an MMN on the WWW. However, when this system is operated around the globe each stable nation state, would posses their own encrypted control code for national security and also have their own security protocols for sensitive data processed by any PFN through TRAC software system and or communicated on the MMNWWW. Data transfer and availability would be governed by it's sensitivity and in some cases would only be handled as it is today on intranets, L band military channels, etc., but still monitored and managed by high security PFNs.

In hostile areas of civil unrest the same world organizations could address and mediate with any warring parties in the same manner they do today to negotiate a peace settlement. However with this technology any agreed upon accords or treaty measures could be written into software programs and downloaded into PFNs with this TRAC software to monitor and remotely control and or use robotics to referee the terms of any agreement. The PFN/TRAC system can be installed and or activated in any and all equipment to help in the processes of nation building to insure fair exchange between the warring parties and to insure any aid efforts are guaranteed to be utilized in the fashion intended. Also the management and control systems can serve to better follow the actual behaviors of the agreed upon hostels with out interfering or intervening or introducing any other new groups (Troops, etc.) or societies directly into a localized conflict.

The PFN/TRAC system can be given a progressive array of tools to help safe guard any agreed upon peace. This technology can give audio instructions in the appropriate language and repeat or site the agreed upon terms when they are violated. This accomplished by the monitoring of improprieties with the hostile parties and or persons. The technology will record incidents on location and in the remote monitoring and control center. It can then aggressively intervene from the authorized monitoring and control centers with varied levels of deterrents all the way up to full lethal weapon deployment and use. All these actions are tracked and stored in memory systems both on board the PFN and redundantly in a plurality of remote locations e.g. (locations or sites agreed upon by the signers of the treaty). Accessory deterrent systems type, application and real-time use can involve all signing parties or leaders simultaneously along with their real-time communication to the involved masses.

In Normal PFN/TRAC operations.

Federal Access and Control Technology FACT, Commercial Encrypted Web products CEW, e.g., TRAC programming or PGP C.O.T.S. products, or Financial Transaction products FTP NCR or the new wireless programs as C.O.T.S. products or TRAC programming, are all the primary programs that are a part of TRAC's secure communication links to any remote management and memory storage computer gateway or node that can network with any host machines ASS sub-programming module. This primary programmable TRAC module software will prioritize communication from the communication links as determined by the standardization efforts for accountable remote control as per application specific protocols and real life social economic and environmental circumstances for this real time management system. Local memory storage and time are both kept as part of the TRAC programmable module as well as, the application specific programs for management and control of society and it's equipment.

The Mobile Management would have application specific programs for remote piloting of a vehicle. (RPV). And most especially this technology's proprietary PASSS program, which stands for proprietary automated slow, stop and secure the vehicle. And the secondary modality of the this proprietary automated shut down PAGSSS proprietary automated guide, slow stop and secure. This of course can in part be accomplished through remote control if so desired. M-ASMP stands for mobile application specific management program. This is any number of basic programs that are now completed by OEM PCMs that will be monitoring vehicle sensors and operating activity controls, as well as, accessory sensors and additional controlled devices made accountable through an interfaced TRAC equipped processor in a PFN. These standard mobile application specific programs will provide service data analytical and repair data, environmental testing and feed back of the equipment numerous forms of tracking and progressively provide guidance telemetry with video and distance sensing, as well as RF telemetry beacons and accompanying algorithms locally and in any interactive highway system or mobile management program operating for PFN contact. These last components are the PGASS equipped programs or more sophisticated systems for total robotics and accountable remote control of mobile assets. Commercial Application Specific Management program C-ASMP is designed to provide specific service data and remote analysis functions, as well as, control any machinery or equipment from at least one remote location and or to shut it down for emergencies or in accordance with any financial arrangement, leasing, taxing, etc. Also, monitored is any environmental data, or any application specific data like fuel or energy use or resource use water, air, etc. Some other general application specific areas for the commercial management

areas are industrial, agricultural and construction. These special programs will run in specific designed PFNs and all the programs may run in universal PFNs. The PFN architecture addresses all the possibilities throughout all the related PFN application stating many numerous configurations and modalities to develop this organizational electrical interface platform and system for better management of the earth's resources and to help all individuals to see jointly how best to interact with each other and their use of technology to sustain and perpetuate a health happy existence for all.

Home Management Program H-ASMP is another application specific set of programs that can offer home nursing telemetry for specific physical conditions, it can be the control center for all utility use and services, it can communicate with short range communication PFN systems as detailed through out the other related patents, provide an interface point for diagnosis and repair of household appliances with FACT and smart card electronics either by short range RF signals or hard wire connectable. Of course these systems can be used for commercial applications in factories to operate an Intranet and perform Internet activities to lessen the cost of transmitting data all at the discretion of the owner or governed by any agreed upon contract or governing authority.

Figure 3

Shows the two basic PFN communication modalities, which are being developed as prototypes. There will be one way transmission devices (basically pagers and RF receivers, including an accessibility to any responsive broad band scan function for the standard AM and FM car radio receiver. With a radios standard seek and scan function initiated by the TRAC PFN software (FACT for example, through this connectable interface) allows law enforcement to give remote commands through the PFN/TRAC processor to perform this technology's PASSS and PAGSSS shut downs and securing of a suspect vehicle. This can likewise be performed by the pager system or any long or short range RF receiver or transceiver on board.

And there will be two levels for the two way transceiver devices. One in the US employing the two way pager systems developed by Motorola, (the reflex products and protocols) and the other more sophisticated using wired telephony technology and or wireless RF equipment and or Cell phone technologies. The varied peripheral capabilities and containment or extended physical protections will be application specific and determined by the modalities used to interface the necessary components to provide an accountable PFN system to comply with any standards effort and current technical development.

PFN structure shape and size will be governed to some extent by the hardware employed.

Some exterior containment might be the same for one and two way pagers and the same for many of the solid and or integrated circuit evolution's and combinations. The containment will house the standardized TRAC Software in a processor and or any and all accompanying IC chip sets for pager cellular phone, RF circuits, and GPS. And or interface any current C.O.T.S. communication products or devices through the modalities detailed throughout all this technology's related patent applications. This versatility will be replaced with universal interfaces, components and structures as a progressive accountable focal node for all automated and remote control functions is created for these specific applications and in the areas on mobile management, home management, commercial management, control security technology.

The drawing also illustrates monitoring, remote control and or management systems from the local level to the global level. This Figure is utilized in other related applications 202 and 300. The 300 network displayed at the top of the Figure three is the basis and structure for 1100 and 1200 series monitoring and control systems. This networking can support this technology's "green eyes" and "spider eyes programs" at varying levels of public involvement and acceptance with varying levels of security, either as part of the Internet or in part as isolated networks interfaced with the web protected behind fire walls. The data and its use will be determined by the public, it's governing bodies, processes and agencies to set the appropriate rules, regulations, laws, specifications, codes and standards, for any Internet and or world wide web engagement and the equipment use. However, this machine messaging network MMN interfaced with the web WWW and utilizing the detailed communication systems of phone nodes, modems RF equipment interfaced with gateway computers can provide all the secure connectability for servers and providers to commercially full fill all the above detailed primary and sub programs desired to be run in a PFN/TRAC module in any manner prescribed by any and all governing laws, rules and regulations to insure accountable remote and automated control and or management. In the top local section 108 or 1208 in the 300 patent application is one remote storage but a plurality of memory storage is possible and probable in many applications throughout any networking.

The Figure also shows all the qualities and peripherals, as well as, the security systems for conditioning any two way transmissions. There is many encrypted C.O.T.S. products to condition a data signal, and this technology will attempt to accommodate any and all hardware embedded software, and software encryption programs as possible to provide greater commercial and security options for any signal from a PFN. The many products will be named in an appendix to this application and the this technology will do everything it can to cooperatively develop joint ventures in an effort to expand this technology and others to

increase world stability through good management of the socioeconomic environmental interaction between man and machine. Humanity will still be the governing control over the PFN/TRAC system through it's evolving nation states however, it will be provided more accurate and real time data in an organized fashion to aid in the appropriate decision making process in the future development of humanity in a more harmonious mode with itself and this earth.

Directly below the monitoring and control net work are two dotted lines representing wireless transmissions. The two directional dotted line on the right represents two way transmissions and has the letters DES on the left side which is an anchormen for Data Encryption Standard and PGP on the right which is an anchormen for Pretty Good Protection. DES is a protected government technology that has specific hardware, for high security data. The software or embedded firmware for the government is handled strictly and provided through the government for their high security applications. This invention would of course be capable of employing this DES security system protocol on all of it's two way transmissions between devices, e.g., PFN's TRAC system computer terminals and or gateways, their wireless and or any land line communications to PFNs. Or to other networked terminals and or any data storage systems that were approved for this type of security system by the government or it's authorized agencies, the Justice department FBI or any national security agencies the Secret Service, CIA and DOD etc. This is being mentioned presently to make clear that the standard PFN and TRAC module will be capable of accepting any DES hardware or software as part of this technology's primary program FACT.
TRAC's Federal Authorized Control Technology.

There are varying levels of DES security presently and FACT's capability by application and use would be determined by the United States governing bodies and agencies, as per the publics empowerment and acceptance for national security balanced with individual freedom and the respect for the individual citizen privacy in the deployment use and functions of any monitoring and or remote control of and through privately owned possessions, such as automobiles. This technology has been designed to provide more organized control and accountability to humanities equipment, machinery and vehicles for the optimal management of the equipment to increase public safety while improving the quality of life for the individual with the respect of privacy. This requires accountability for the collection and use of PFN/TRAC data and or any other parallel remote control and monitoring technologies. The use of these technologies have to have the best temper proof measures and the strictest criminal and civil penalties for any miss use or abuse of data; either collected or dispersed in a reckless and or negligent manner. For these technology's to better humanities quest to better

itself and it's total survival these technology's need to be structured and standardized in accordance with society's law and order and in the case of the United States tailored with respect for the individual's privacy who is continually ask to compromise more personal privacy with any and all data acquisition to provide more improved and better services and which require more enhanced knowledge.

Once again this technology address these issues as it's nature and scope claim and as a necessary and correct approach to provide responsible and accountable aggressive remote control, monitoring and robotics. In this effort this technology seeks out all parties commercially, governmentally, socially, environmentally, and financially to address the issues and form joint ventures to achieve sound safe guidelines that marry up well with society to develop these technologies and to evolve the economic tool to better value and reflect all aspects of equipment use and to improve safeguards to all such transactions.

As mentioned earlier there are many types of encryption protocols for security. PGP is the commercial versions of encrypted data. And as explained earlier there is a great number of such systems that can afford reasonably good protection for many security programs. Some of these are just software down loads and can be part of the software in a PFN/TRAC system and capable of running an encryption program piggy backed through other servers signal conditioning software. As detailed earlier the primary programs software will delineate restricted data from unrestricted data if so desired and this capability exists for DES with hardware chip sets and embedded software or firmware, as well as, solely performed by software programs. With both DES and PGP both ends of the transmission must be equipped to electronically cipher and decipher through a encryption and de-encryption key program no mater which technology is used and in what form of hardware, hardware embedded software firmware, or solely software added to any existing hardware either in the processor or computer section of a PFN, it's modem circuitry, and or as part of any of any of it's communication devices circuits and or any remote monitoring control management and storage system responsive to any PFN/TRAC unit.

These security protocols for the highest security have to be maintained in every transmission including throughout the 300 network for wireless and land wired systems and this is why the phase "Same Security Protocols" (with arrows) parallels the horizontal 300 network labeled world, local and sectional. Sectional represents states, or areas of close coordinated areas.

The basic reason the encryption protocols are only shown on the two way transmission PFNs is, because, they could be broadcasting secure installation video and other sensitive telemetry data. It may not be as necessary to protect one way directional remote

control communications in all security applications or in many of the management applications, because, there will be less of them transmitting data back and thus more difficult to Figure out their purpose or instructional command codes. However, in the highest of security applications signal encryption may be required as well, for one way command level remote control, and therefore is shown as a possibility in drawing 4 number 403.

301 is the two way communication device with the DES and the PGP systems on each side showing the options of encryption and the small arrow to the right of PGP points to the right block as a 2 stage memory on board the two way PFN, which are parts numbered 105-107 in Figure one. Number 302 is a line list of possible accountable functions for full remote control and remote monitored robotics. At least one variation of this two way PFN will completely support all of these functions including any special sensors, identification systems environmental sensors, audio video systems, all machine controls and will monitor all machine sensors. 301 memory storage are shown here as a plurality of local memory. One a current running loop of application specific determined length and content. And the other local memory a application specific incident based or event storage. This second data storage is permanent and housed in a protected area with special authorization necessary to physically and or electronically to access the data. The proprietary design, also, provides either a redundant storage of this same incident in at least one remote location or a limited message flag (for the data limited two way pager systems) to be sent to an appropriate authorized monitoring E-mail address, or computer network or RF receiving node. While these memories are detailed in a plurality for local and remote locations this is merely done to provide these options for any standards effort that can be applied to the application specific protocols and areas.

303 points to the simple one way receiver PFN. The dotted line coming down from the top depicts the one way communication for one way remote control of equipment. However, 303 also can support the same two stage local memory storage. With this one way system, there is no wireless remote storage, without the physical removal of the data or through physical connections. There is no report back function in real time. The one way system can also support the same processor capacity to do all the same functions as the more sophisticated two way PFN, but is limited in remote control by not having a real time monitoring in a remote location to guide tasks by video. The 303 one way system must have it's data recovered physically through a secure download communication port. This interface communication port can, also, be in place on the two way PFNs if so desired. However, remote control functions can be preprogrammed and or guided and or confirmed through other two way PFNs on location that can video the one way PFN systems host and or report

on other telemetry data about the one way PFN that warrants specific remote commands. So by teaming one and two way PFNs one can provide a complete remote control system for the one way PFN. Total accountability is still provided in two levels in the one way PFN (re-writable and permanent). Also an extendible and retractable connector either hydraulic, air or electrically activated and controlled can connect the one way PFN to any of the communication ports on same equipped two way PFN to report back any pertinent data that needs near real time consideration. In fact in a security setting only one two way PFN mobile device could recover data from all the inexpensive one way PFNs and report it back to the remote monitoring and remote control system. This mobile two way PFN could also accompany any one way PFN to give report back data for real time remote control of the one way PFN equipped machine whether it was stationary or mobile one way PFN.

304 Illustrates all the same functions that are listed for the two way PFN and states that it has only a physical retrieval accountability for any data stored. 305 is a block at the bottom of the page and its functions can be performed by both the one and two way PFNs. 305 is any special sensors section that will be gathering application specific data for these any applications e.g., environment, radiation counters that transduce the number of Rads or particle strikes into an electronic signal for the processor software to evaluate through compare lists set up for an application specific PFN or as burned in firmware on simple device where a simple PFNs is set up as to sense an environment. If this PFN is at an installation or in a remote location it will be powered by solar cells to recharge it's batteries. 305 special sensors will be many different applications specific sensors that send an electrical signal to applications specific software programs in the PFNs. The TRAC system will be programmed special to handle specific functions for specialized sensing, e.g., like hydraulic weight sensors. many of these peripheral devices and sensors exist as C.O.T.S. products and their are flexible software products that can be easily adapted to support these applications.

Another 305 special sensor is the nose. Which is a sensor that can identify odors 2000 times more accurately than the human nose and is capable of discriminating substances and matter at a molecular and even atomic level. This sensor already designed to deliver unique electronic signals for it's application specific software compare list library of known substances will serve well in high security applications to identify biological and chemical toxins explosives, e.g., potassium nitrates etc., and leaks in regular chemical containers in any commercial or governmental installations airports. And when coupled to a mobile PFN/TRAC system preferably a two way PFN on a host machine full accountable robotics can be provided for most any hazardous environment and or contraband search task. As mentioned earlier, the PFNs could operate electrically controlled weapons in unmanned

equipment that was damaged or unmanned either due to the loss of life or to prevent the loss of life by using the machinery and equipment through remote control and or full robotics (based on the level of PFN computers and onboard programming). The options are vast and varied to improve security and safety for all facets of remote control protocols. To help world order and nation building by monitoring equipment and material movement, while robotically controlling terrain and police an area for aggression, without risking mediating personnel any more than is absolutely necessary. (To help enforce treaties so that the assignees and their constituents are on the same dotted line with the non emotional objective cold hard steel equipment that stands fast to the terms that have been agreed upon. Once again, audio recordings would be in a native language which can be remotely sent as precursors to any physical intervention. First as a persuasive protocol, e.g., water cannon, gas, rubber bullets and all the way to a final lethal weapon activation a last resort to save lives and preserve a peace accord). These PFN armored machines and or equipment would be all terrain like tanks, track vehicles, hum versus wheeled vehicles, hover crafts, etc. And of course their peripherals could be all of the same and more in the military weapons categories. Eventually special peace keeping PFN controlled equipment would be created to help maintain order in an unstable area (This is a system of MM Network to develop a Real ROBO Cop in plurality, through this technology's Spider eyes program) but first as part of every piece of equipment networked and remotely controlled.

Recently the "car plane" designed by Moller has been developed for future three dimensional transportation for the individual. The technology exists to day to set up a guidance systems with the three coordinates delivered by the current GPS systems. Their is latitude longitude and elevation and when used with the military's accuracy achieved with an additional correction signal for the ionosphere distortion of satellite signals the GPS accuracy is within centimeters. So most probably this invention will see government use for a while before it is a general public individual transportation tool. In any case the FAA could more readily organize and develop the car-plane technology with this invention. And the PFN will be invaluable in consolidating the accountable black box, communication systems and locating equipment all in one concise system that is easily tailored for monitoring and controlling an ever increasing numbers of these car planes in the future. Basically all the transportation systems will be coordinated in computer network to micromanage out collision possibilities in any plane of travel, and the PFN/TRAC system is an ideal system to organize and initiate this effort for present travel and the next millennium.

Figure 3A

This Figure is self explanatory in the properties of the most generally used communication devices in the PFN/TRAC system. However a brief review of the cart can help to better understand the use of the devices and guide their use in application and standards consideration. The left side column is the communication devices them selves. In reading down this column there is one way paging,one way radio frequency signal equipment, two way paging, two way wireless phones and land wired PFN's listed as PHONE, two way radio frequency signal, and cordless phones which are short range radio frequency signals received and put out on land based phone lines. And finally short range radio frequency signals. However at the very bottom is a definition of letters describing the functions of each of the communication devices, what they can do and therefore be used for in the PFN applications. Each PFN will have at least one communication device interfaced with a processor system and memory storage

R = RECORD

r = REPORT

O = ONBOARD

RR = REMOTE RECORD

mc = MINIMUM CAPACITY

LD = LIMITED DISTANCE

Across the top are activities performed by the PFN such as audio/video data gathering, machine activity controls and telemetry, personal or operator telemetry, environmental telemetry. By using the letter key provided it is easy to see the properties, qualities and capabilities of the one and two way PFN systems and determine the best type of system for any particular application. This chart can be referred to when reading and reviewing Figures 3, 4, 5, and 6 with all the different types of communications detailed. This chart will quickly provide the basic on board record and report back properties and data storage options that can be expected from any particular type of PFN by the communication devices they are employing.

It is important to remember that at the time this invention has been conceived that a standards effort and FCC approval for dedicated frequencies as well as specialized repeating or automated digitpeating for short range Rf signals as well as the protocols for using other wireless telephony devices and systems, e.g., pagers and cellular as well as satellite systems have not yet been determined. This is why all the possible communication devices are named and because some application specific PFNs will use at least one of them including any of these listed in Figure 3A as well as other specialized frequencies detailed in other related PFN

applications, and also because many universal PFNs will be responsible for interfacing all of 3A's communication systems plus more to complete the flexible receptive mobile PFN web structure to provide repeating or digitpeating functions for mini or micro PFN trans-ponders or personal PFNs, which can use low power and limited range transmission equipment. Either to communicate in a a close circuit intranet or encrypted Internet or through IP gateways, e.g.,other PFNs to any other from of communication equipment desired, either isolated encrypted, etc., or even for public or community viewing.

Figure 4

This drawing is of the simplest one way communication PFN and these basic electronics have already been prototype used and proven from and for the other related applications. Basically with the one way communications there is data storage on board the host in the PFN at two separate locations, but they require physical retrieval of the data. This device in it's most basic form will not report back to any remote control and monitoring system, but can be sent messages, which will activate preprogrammed responses. This is the basic encryption of a one way PFN, but, as was earlier described in Figure 3 these units when used in concert with the other two way PFNs can transfer their data and thereby have the two way PFN report the data to a remote location. It also should be noted that this can also be accomplished though a land line comport available to a one way mobile PFNs (provided it is outfitted with the proper DET data encrypted terminal as part of the land line connection or a one way PFN out fitted with DES chips. Of course the same would be true for secure commercial applications as well with PGP protocols. All that is required is the extendible and retractable connector developed as a variation of the tow bar coupler and electrical connector described in the third related provisional application 112756-300. RE. Interactive high way car towing, car trams or car trains which is the energy efficient individually private mass transit option for land based vehicle platforms in long distance travel.

Also another and more efficient transfer of this data from one and two way pagers for longer messages, which will not require expensive hardware is the infrared comports that have been extensively detailed in the other related applications and or light transmissions or the short range RF transceivers. These systems are used with law enforcement and or secured installations and or stationary commercial settings for industry, etc., for the PFN/TRAC system

To follow the flow of the one way systems in Figure four,300 block of boxes is the world wide sectional and local network gate ways to send data to the one way PFNs as indicated by the thin dotted arrow passing between the wireless transmission box and the

security level 403 DES/PGP box. The question mark in the 403 box is there because it is optional security for one way transmissions into a secure installation as was discussed earlier. Looking down from the top center block labeled 200-204 PFN containment is a series of boxes which are all components of the PFN. These components described here are all individual C.O.T.S. products that can be interfaced as separate devices or IC C.O.T.S. components integrated and connected or hard wired together or as combinations of devices and IC components to provide the hardware to support TRAC software. The invention has it's own proprietary configurations that are detailed in many different modalities throughout all the related filings. And the invention's PFNs and TRAC remote control system is capable of interfacing with many other already existing components and systems to enhance any remote control product and for security and management. This invention was and always has been expressly designed in this manner to provide a secure physical platform and electrical interface to focus, organize and help standardize remote control functions for all equipment in every application. The TRAC software protocols are designed to continue this security and provide accountability to the system from the PFN to any network the system is interfaced with. The invention's TRAC programs can be a stand alone products or set of interfaced devices which can be married to any existing system (modular) and add to both creating a better set of products and or better remote control, management and monitoring systems.

To the right 400 is the standard pager as one of the one way receivers and this circuitry is detailed in the first patent. 401 another one way option receiver could be any type of radio receiver on any frequency and all the frequencies are listed in the 60-108 related patent. 402 is a combination of communication and processor functions integrated and combined into one system and a specific C.O.T.S. product made by Motorola Corporation, called "Create-a-Link" and is one product that serves as a prime example of the inventions versatile application in utilizing other technologies as part of the protected interface and accountable data storage components rather than this proprietary pager technology and parallax mini computer if so desired. Of course the TRAC protocol would be programmed into the Motorola software or firmware to authorize software commands, authenticate remote control activity and store it in the appropriate storage. And for certain applications this might be part of an ideal configuration for some application specific PFNs if the functions did not require great amounts of report back data to remote locations.

The mini computer box directly below, the C.OT.S. receiver processor (Create-a-Link or comparable device is for the traditional PFN computers either the Basic stamp computers I, II or the planned Euro-boards 188, 386 and 486 or even those with Pentium processors, that were described in the earlier patent 112756-202. The choices of computer processors is once

again application specific with the 386 or higher processor being necessary to support better quality video applications with reasonable speed, smoothness, and quality, for digital applications. However, snap shot video applications can be achieved with smaller and less capable processors. The mini computer's the first sacrifice in any real time full video being jerkiness and or the time needed to process the digital image.

However the first prototypes are planned for analog video systems and simple processors to prove feasibility and the digital systems will accompany the more sophisticated minicomputers and special TRAC programming. This can lower video and audio cost for these applications but, will be more costly in the processor system in the beginning. These first video systems will document cabin activities and external activities, and then evolve as an intricate guidance tool for automated and remote control guidance. To use video to aggressively remotely control a vehicle and or drive it through automated activity controls it will require extra sensors as to steering parts position speed and the activity controls on the acceleration and braking functions to effectively and remotely control a machine in real time. And other criterion is video quality and properties especially for the report back function which will determine the capability and speed of the vehicles that can be managed through remote control operations. The on-board communication systems, e.g., cellular or wireless phones, two way reflex paging and other RF transmission equipment either on board the host equipment and controlled through the PFN and the accountable software TRAC that must manage the authorization of a signal and authenticate any command functions, as well as, process all the sensed operational and driver action data and store it in the two local memories under the proper circumstances with the appropriate time date and command string record.

As detailed earlier for the two way pager systems and limited remote data transmissions they will be assisted by other more sophisticated PFNs that can be utilized in conjunction as (shepherds or watch dogs to better provide visuals for any of these less capable PFN units that have limited, or restricted report back or video quality due to limited data quantity capability especially in reporting transmissions as is the present case for the two way paging system Create-a-Link II (a Motorola Reflex protocol) or as depicted here a total lack of any on board wireless report back functions, because this is only a one way (pager) receiver as it is configured in Figure 4.

To the right of the mini computer box is the little box GPS number 407 and it is the global positioning system or it can be any type of locating equipment either a separate hand held device interfaced with cables or as an integrated chip set circuit hardwired into the computer or processor, or as merely a chip set as has been described in 112756- 202. The last two of which can also be in the form of cards with edge connectors that plug into the euro-

board 100 mini computers detailed in the second patent 112756-202 as mentioned above and incorporated herein by reference. These would be the hardware components to run the TRAC programmable authorization and authentication as well as, operate and manage the record storage and provide hot geographic coordinates and time synchronization data or confirmation for the local TRAC module clock.

The HPC box to the left of the mini computer box is the Host machines Programmable Computer or control circuit and or processor. This can be the only computer in the secure interface or it can be interfaced with other control circuits or processors either proprietary and or other C.O.T.S. products which are coupled in the secure interface and made a more reliable, accountable monitoring and remote control device termed a PFN which stands for (protected) Primary Focal Node. The PFN is designed specifically with versatility to provide a physical platform with a universal electrical set of interfaces and accountable TRAC software to develop a logical organization and manageability for remote control and robotics to meet societies legal needs for all these related technologies and their combined functions. This focal point (PFN) on each piece of equipment housing and linking all electrical control circuits with host peripherals and sensors to off board monitoring and remote controls provide the organization, security and accountability through TRAC software and memory storage for society to meet insurance and security concerns for the use of aggressive remote control and robotics. And above all the PFN and TRAC gives organization and structure to write a standard to for remote control and robotics applications for all possibilities. The PFN/TRAC system combines and focuses communication control circuits and data storage in one safe and secure accountable local location so that DOD, DOT highway safety agencies, FAA, FCC, FBI, CIA, law enforcement professional organizations, e.g., IEEE, and the many industry standards and watch dog groups can form a standards effort with the major auto manufactures and equipment and machine manufactures in every possible area. The invention has been expressly designed to help create a responsible organized modality to this emerging area of merging technologies and help to marry it well to societies laws and needs.

To the left of the HPC block there is the host equipment interface which would be merely a multi-pin interface connector from the box if the HPC is contained with in the PFN. The lower blocks below 404 is the sensory or telemetry data gathered on the machine and or operator, and the box to the right represents the functional control of devices or accessories on the host equipment. With these two functions combined the equipment operation can be achieve through remote control and monitoring all as part of an entire network.

Returning to the center of the page and specifically the lower center their is three

boxes displaying the two levels of on board memory storage with three accompanying numbers 105, 106, 107. These numbers are used to delineate the different types of memory storage devices and not the actual number of devices employed in any specific PFN system. The reason the numbers are used is because these are the present day prototype developments and are listed as present technology, however, due to the vast improvements in memory capacity with all the many different technical variations the invention does not limit its claim to these specific devices and systems that might be employed into this secure PFN, the secure and accountable TRAC interface.

405 Points out that these data storage components and in fact all the PFN devices and components are detailed extensively in the previous patent 112756-202. However the planed universal prototypes in the security area will be detailed presently as to the proprietary devices components and system functions excluding application specific configurations (software) TRAC for Trusted Remote Activity Controller.

406 shows that the data retrieved from a one way PFN is done through physical contact unless it has an IrDA communication port or short range RF transmitter.

408 is TRAC the programmable and modular software and varies in structure and format based on the different hardware implementations weather it is C.O.T.S. based, PC, Programmable Controller (Stamp); or if it is custom, logic sequencer, micro processor, FPGA (field Programmer Gate Array) or a custom gate array. Even though these are not all displayed in the three Figures in this application all of these hardware options will probably run some for of TRAC software in some application and therefore should be included as hardware implementations for this technologies PFN/TRAC

These TRAC Interfaces/Software will have algorithms for BANK/Stock Exchange Transaction Products. Many of these will be supported C.O.T.S. products and through the primary TRAC software. There will be other accountable programs for remotely piloted vehicles RPV and this technologies proprietary PASSS software for the automated slow stop and securing of a vehicle in a stationary position. And this technologies PAGSSS software which has numerous variations but basically it is the proprietary automated guidance slowing stopping and securing of a vehicle through remote control as an evolution of PASSS. Other software specifications include the use of a Commercial:128/64 bit Encryption for web transactions. And for high security in government and military applications: DES the (Data Encrypted Standard).

The interfaces and connectors are named extensively in the related patents however, presently the Automobile industry is planning to start a standardization effort for electrical connect-ability of accessories. This technology has been focused on this point or issue in the

last two related patent applications and looks forward to participating in any effort to develop H-Rel universal electrical connectors, and can offer actuators, sensor protocols, signal levels in the aggressive automated and remote control devices to reach deeper into a standards effort in this area. This technology will be constructing prototypes with these interfaces anyway and a collaborative effort is always welcome when ever possible. Telephony is another industry interface with digital cellular, PCs, 56K modem, pager technology as well as the varied RF signal and light transmission equipment.

Figure 5

This an illustration of the simplest two way communication systems and the necessary security devices to condition the signal encryptically for security protocols. It is basically another flow chart showing the data from the remote control and monitoring network, as well as, all the data and control signals to the data storage and the peripherals through the many possible processor options running a form of TRAC software. This is the same as Figure 4, however, it is in two directions with the remote control and monitoring system and there by creates three accountable levels of data storage on and off the host piece of equipment. Two levels on the equipment and at least one partial storage remotely copied of any pertinent data. Or an application specific Email or warning flag detailing the PFN/TRAC systems ESN electronic serial number to obtain physically a more extensive memory record of an event or incident.

This drawing is of the simplest two way communication PFN and these basic electronics are planned prototypes from and for the other related applications. Now with these basic two way communication capabilities there is data storage on board the host machine in the PFN at two separate locations that still can be physically retrieved; but, also the capability to report this data to at least one remote location (is limited). This device in it's most basic form will report back 20 characters to a remote control and monitoring system, through a reflex paging service in the U.S., South Central America, middle east, and Asia. It will also be possible in the future to accomplish this in Europe with the ERMES version of two way paging protocols in the near future. And these messages can be sent to E-mail addresses for inexpensive world monitoring management and control.

And of course any of the two way pagers can be sent messages, which will activate preprogrammed responses as is the case with one way paging. This is the basic description of a two way paging protocol PFN, but as was earlier described in Figure 4 and Figure 3 these units when used in concert with the other two way PFNs with more sophisticated) transmitters and or land line DETs Data encrypted terminals can transfer more of their data efficiently to a

remote locations. Also, preprogramming in the PFN computer can send a series of 20 character messages to a remote location, where the monitoring software can reconstruct the whole message. Another option is multi-paging devices that can be combined to send a large data message with different carrier frequencies for each paging device. This would increase the difficulty in intercepting the entire signal or message being reported. (Motorola's reflex two way paging protocols are being referenced here for all of these options basically, the ERMES products are still under development.)

And to reiterate these two way PFNs can also accomplish data transfer though regular land line comport connections where ever available provided the PFN is already out fitted with DES chips or PGP software for it's wireless transmission capabilities. (If not it will have to send it's data through a local DET comport which will probably be hard wired to the local monitor and remote control station or network gateway). All one and two way PFNs will be capable of generating dial up phone tones to connect to a phone node if so desired. And of course if land line connections are available for HS and MS security they will have the necessary sending and receiving equipment and software to handle the encrypted signal. Of course the same would be true for secure commercial applications as well with PGP protocols. This could all take place in an automated setting as well. All that is required is the extendible and retractable connector developed as a variation of the tow bar coupler and electrical connector described in the third related provisional application 112756-300. RE. interactive high way car towing, car trams or car trains which is the energy efficient individually private mass transit option for land based vehicle platforms in long distance travel. The same communication coupler that link all the PFNs in each vehicle to control which power plants will increase the collective power to increase the speed of the train.

To follow the flow of the two way systems in Figure 5, 300 block of boxes is the world wide sectional and local network gate ways to send data to the two way PFNs as indicated by the thin two directional dotted arrow passing between the wireless transmission box and the security level 503 DES/PGP box. This 503 box is there because it is a necessary security for any two way transmissions out of a secure installation as was discussed earlier.

Looking down from the top center block labeled 200-204 PFN containment is a series of boxes, which are all components of the PFN and housed within the containment. These components are all individual C.O.T.S. products that can be interfaced as separate devices or IC- C.O.T.S. components integrated and connected and or hard wired together to form combinations of devices and IC components. The invention has it's own proprietary components and configurations that are detailed as many different modalities throughout all the related filings. And the invention's PFNs and remote control system is capable of

interfacing with many other already existing components and systems to enhance any remote control product and or security system in many ways. This invention was and always has been expressly designed in this manner to provide a secure physical platform and electrical interface to focus, organize and help standardize these functions for all remote controlled equipment for every application. The invention can be a stand alone device and or system of any size (or a set of interfaced devices systems and networks) or it can be married to any existing system and add to both by creating a better set of products capabilities and remote controls in any monitoring system as well as provide accountability through the TRAC software.

To the right 500 is the standard two way reflex pager as one of the possible two way receivers. 501 another two way optional transceiver, which could be any type of radio transceiver on any frequency and most all the frequencies are listed on Figures 9 and 10. However, the allocated and dedicated frequencies are designated and many of them are shown on the allocation chart. These of course would be the ones used for the government and other high level security protocols however as has been stated the pager and wireless phones can be commercial grade frequencies accompanied with encryption technology for security. For this reason other low cost public airway can be utilized with the these same security protocols. 502 is a combination of communication and processor functions integrated and combined into one system and is a specific C.O.T.S. product made by Motorola Corporation, called "Create-a-Link II". This all in one product serves as a prime example of the inventions versatile application in combining other technologies as part of the protected interface and accountable data storage components, when ever possible, rather than solely relying on the proprietary pager technology and parallax mini computer and other proprietary computers if so desired. And for certain circumstances this might be part of an ideal configuration for some application specific PFN's. This Motorola product "Create-a-Link II" is different in that it employs the reflex two way paging protocols which are a necessity to achieve the report back function for this minimal two way variation.

In the drawing the mini computer box directly below, the C.OT.S. Receiver processor (Create-a-Link or comparable device) is for the traditional PFN computers. Either the Basic stamp computers I II or the euro boards 188, 386 and 486 or even those with Pentium processors, that were described in the earlier patent 112756-202. The choices of computer processors is once again application specific with the 386 or higher processor being necessary to support full video applications with reasonable speed, smoothness, and quality, however. Snap shot video applications can be achieved with a smaller and less capable processors in the mini computer with the sacrifice in any real time full video being jerkiness

and or the time space needed to process any digital image. This condition requires extra sensors to effectively and remotely control a machine so equipped in near or very near real time. And other criterion in video quality especially for the report back function is the level and capability of the on board communication systems, e.g., cellular or wireless phones, this 2 way reflex paging and other RF transmission equipment either on board the host equipment and controlled through the PFN. Or assisted by other more sophisticated PFNs in the network and or on location that can be utilized in conjunction as (shepherd systems or watch dogs to better provide visuals for any of these less capable PFN units that have limited, or restricted report back or video quality due to their capability to handle the quantity of data required, especially in reporting transmissions as is the present case for the two way paging system Create-a-Link II (the Motorola Reflex protocol), which is best set up to report back in a limited snap shot of images. However much other report back data from other sensors can be provided a good and reasonable form of communicating their data back to at least one remote location.

To the right of the mini computer box is the little GPS box number 507 and it is the global positioning system or it can be any type of locating equipment Lorands, etc., either a separate hand held device interface with cables or as a integrated circuit hardwired into the computer or processor, or merely a chip set as has been described in 112756-202. The last two of which can also be in the form of cards with edge connectors that plug into the euro-board 100 mini computers detailed in the second patent 112756-202 as mentioned above and incorporated herein by reference.

The HPC box to the left of the mini computer box is the Host machines Programmable Computer or control circuit and or processor. This can be the only computer in the secure interface or it can be interfaced with other control circuits or processors either proprietary and or other C.O.T.S. products which are coupled in the secure interface and made a more reliable, accountable monitoring and remote control device termed a PFN which stands for (protected) Primary Focal Node. The PFN is designed specifically with versatility to provide a physical platform with a universal electrical set of interfaces to develop logical organization and manageability for remote control and robotics to meet societies legal needs for all these related technologies and their combined functions. This focal point (PFN) on each piece of equipment housing and linking all electrical control circuits with host peripherals and sensors to off board monitoring and remote controls provide the organization, security and accountability to justify to society and meet insurance and security concerns for the use of aggressive remote control and robotics. And above all the PFN gives structure to write a Standard (for remote control and robotics applications by focusing communication

control circuits and accountable data storage into one safe and secure location. DOD, DOT highway safety agencies, FAA, FCC, FBI, CIA, law enforcement professional organizations, e.g., IEEE, and the many industry standards and watch dog groups. The invention has been expressly designed to help create a responsible organized modality to this emerging area of merging technologies and help to marry it well to societies laws and security needs.

To the left of the HPC block there is the host equipment interface which would be merely an interface connector from the box if the HPC is contained with in the PFN. The lower blocks below 504 is the sensory or telemetry data gathered on the machine and or operator, and the box to the right represents the functional control of devices or accessories on the host equipment. With these two functions combined the Equipment operation can be achieve through remote control and monitoring all as part of an entire network.

Returning to the center of the page and specifically the lower center there is three boxes displaying the two levels of on board memory storage with three accompanying numbers 105, 106, 107. These numbers are used to delineate the different types of memory storage devices and not the actual number of devices employed in any specific PFN system. The reason the numbers are used is because these are the present day prototype developments and are listed as present technology, however due to the vast improvements in memory capacity with all the many different technical variations the invention does not limit its claim to these specific devices and systems that might be employed into these present day PFN secure interface systems. It is equally important to remember that the technology has been and always will be engineered for both backward and forward technology interfacing, as well as, provide the present day technical options

505 points out that these data storage components and in fact all the PFN devices and components are detailed extensively in the previous patent 112756-202. And other related patents. However, the planed universal prototypes in the security area will be detailed presently as to the proprietary devices components and system functions excluding application specific configurations and any specific secret (software) protocols.

508 is TRAC the programmable and modular software and varies in structure and format based on the different hardware implementations weather it is C.O.T.S. based, PC, Programmable Controller (Stamp); or if it is custom, logic sequencer, micro processor, FPGA (field Programmer Gate Array) or a custom gate array. Even though these are not all displayed in the three Figures in this application all of these hardware options will probably run some for of TRAC software in some application and therefore should be included as hardware implementations for this technologies PFN/TRAC.

These TRAC Interfaces/Software will have algorithms for BANK/Stock Exchange

Transaction Products. Many of these will be supported C.O.T.S. products and through the primary TRAC software. There will be other accountable programs for remotely piloted vehicles RPV and this technologies proprietary PASSS software for the automated slow stop and securing of a vehicle in a stationary position. And this technologies PAGSSS software which has numerous variations but basically it is the proprietary automated guidance slowing stopping and securing of a vehicle through remote control as an evolution of PASSS. Other software specifications include the use of a Commercial:128/64 bit Encryption for web transactions. And for high security in government and military applications: DES the (Data Encrypted Standard).

The interfaces and connectors are named extensively in the related patents however, presently the automobile industry is planning to start a standardization effort for electrical connect-ability of accessories. This technology has been focused on this point or issue in the last two related patent applications and looks forward to participating in any effort to develop H-Rel universal electrical connectors, and can offer actuators, sensor protocols, signal levels in the aggressive automated and remote control devices to reach deeper into a standards effort in this area. This technology will be constructing prototypes with these interfaces anyway and a collaborative effort is always welcome when ever possible. Telephony is another industry interface with digital cellular, PCs, 56K modem, pager technology as well as the varied RF signal and light transmission equipment.

Figure 6

Shows a system that can support the most sophisticated high security and two way communication capability for full real time audio/video with either cellular or digital phone or any other comparable radio frequency equipment specially delegated for these purposes (either military controlled and or operated, or a joint venture of commercial and governmental support, e.g., COMSAT commercial satellite.) No matter what ever, even if the commercial wire and land based phone technologies are utilized all will be provided either EDS or PGP encryption protection for medium and high security applications. This most sophisticated machine messaging PFN is being prototyped to support and report every data signal sensed and provide any aggressive remote control for any devices by previously described proprietary technology and or versatile interfacing with other technologies. However, the cost will be proportionate to the level of sophistication and the amount of hardware, firmware, software, and peripherals required or desired.

Even the least expensive one way PFNs can be ordered to activate or deactivate as well as control varied performance of what ever they are connected to. So the system cost can

be greatly reduce by using the less expensive (page type) one and two way PFNs where sophisticated real time video is not required form the remote control unit itself. However these costs will certainly be reduced with these systems being utilized in vehicles for guidance in automated highway systems. But the present lower cost PFNs can still be utilized to wage an aggressive response where all friendly life has been removed from an environment, installation, machinery and or vehicle if the extreme need exists to take radical action. Any standard or specially installed accessory can be remotely controlled. From terminating the use of a piece of equipment by standard means, to energizing airbags on a terrorist, to totally terminating a piece of equipment in a hostile situation through extraordinary means (by PFN detonation's, of explosives etc.)

As mentioned earlier just one mobile sophisticated PFN in most cases. (As the shepherd or watch dog unit can supply visual data to any remote monitor and control terminal). The more sophisticated the watch dog unit the greater the protection of the sophisticated unit. This system can and should be armored and capable to support aggressive weapons, e.g., surface high current capacitor shock equipment systems, laser and electromagnetic wave weapons microwaves, sleeping agents, tear gas, water cannons, pepper spray, tazor gun, net mortars, rubber bullets and convention automated machine gun, cannon and explosives for the extreme security scenarios. Of course the host platform will dictate some of the conditions and restrictions to support any of these devices as well as any real need for any of these aggressive protective defense devices. Identification systems can be employed to recognize friendlies when they arrive and can take orders directly form them on location if need be. This can be accomplished through any and all forms of the short range communication systems already described that can even differentiate friendlies from aggressors during a security incident or emergency with the technology already described throughout all the related patents, e.g., IrDA, limited transmission RF devices other light transmissions and the phone system or any other RF transmitter (which will be personally coded device communicators limiting access by finger print or one of the many other Id systems previously detailed). In the third formal 112756-301 all the electronic devices that are to be controlled on any piece of equipment machine and vehicles, will have a section that specifically describes these security devices for aggressive protection and retaliation options.

Because these devices will in many cases be part of regularly needed host equipment and naturally camouflaged and incorporated into their structures their appearance will be a natural and peaceful one, while harboring a great capability to provide varied levels of aggressive security with the least amount of friendly personnel in harms way. This system for high security automated aggressive response will be known as the Trojan Horse defense

System ("THS"). And will have as a final option for every security PFN in the system a self-destruct order protocol to secure any violated security area where there are only aggressors left. And this final option can be initiated form any where in the world with the correct encrypted secure codes held by the responsible authorities. These TRAC systems of course would have special considerations and guidelines set up for governmental and national security agencies, as well as, world organizations involved many of the most extreme PFN utilization's like TRAC's THS.

The Protected PFN data storage would support any reported record to justify any such decisions and their should be well established procedural protocols for these security scenarios for, e.g., embassies, military installations, nuclear facilities, and any special security risks etc.

All monitoring for every condition in these high security environments would be greatly enhanced and response time to any event or emergency would be almost immediate with accurate data on exactly what transpired to analyze and remedy any same negative situation in the future and or to prosecute any impropriety that transpired

This drawing is of the most sophisticated two way communication PFN and this electrical configuration is the basis for all prototypes in every application no matter the level of security. The only thing that changes besides DES hardware is the specific TRAC–ASS programs like THS. These downloads can be performed on standard manufactured equipment to provide security control through PFN/TRAC system for any rapid deployment need. All the components are and will be proven and in most cases C.O.T.S. products in use presently. Basically with the two way communications there is once again data storage on board the host machine in the PFN at two separate locations, that can also be physically retrieved. However, these PFNs and TRAC software will have full report back capability on their own for every data stream to any desired remote control and monitoring system. And they are also capable of retrieving data from any less capable PFN as earlier mentioned and reporting their data back to the monitoring and control centers. This is accomplished through physical connections or IrDA communication ports and or light or RF transmissions as has been detailed throughout the related patents. Once again all that is required for the physical coupling is the extendible and retractable connector developed as a variation of the tow bar coupler and electrical connector described in the third related provisional application 112756-300. RE. interactive high way car towing, car trams or car trains which is the energy efficient individually private mass transit option for land based personal vehicle platforms in long distance travel. Of course the infrared comports that have been extensively detailed in the other related applications and or any of the light transmissions and or RF signal

transceivers will once again reduce the hardware needed to complete the interface and any data transfer. (But what ever the transmission be physical or wireless of any type; the modality will have to be assessed for it's vulnerability to access any signal and or transmission and the appropriate DES-PGP and or any other security protocols will have to be in place at either end of any data transfer if deemed warranted) as part of TRAC for the very high security protocols commercially and militarily. This focus on the high security protocols was done to show peripheral accessories however the same PFN/TRAC system will be used in everyday applications with out DES and other high security protocols. The exception here is TRAC's FACT program that might carry some high level security control encrypted Commands to allow the proper authorities to control any equipment in a state of emergency. This of course will be determined by the public and it's governing bodies and agencies. The PFN/TRAC system is designed for all accountable aggressive remote control scenarios and the control security is just one of many.

To follow the flow of this two way sophisticated system in Figure 6, 300 block of boxes is still the same world wide, sectional and local network gate ways to send data to all the PFNs as indicated by the thin dual directional dotted arrow passing between the wireless transmission box and the security system box 603 DES/PGP box. The 603 box is there because it is an obvious security necessity for any two way transmissions into and out of a secure installation as has been discussed earlier. With constant transmissions sent out of the compound it would be far easier to obtain critical data to remotely control these PFNs without the Data Encryption.

Looking down from the top center block labeled 200-204 PFN containment is a series of boxes which are all components of the PFN. These components are all individual C.O.T.S. products that can be interfaced as separate devices or IC C.O.T.S. components integrated and connected or hard wired together or as combinations of devices and IC components. The invention has it's own proprietary configurations that are detailed in many different modalities throughout all the related filings. And the invention's PFNs and remote control system is capable of interfacing with many other already existing components and systems to enhance any remote control product and or security system in many ways. This invention was and always has been expressly designed in this manner to provide a secure physical platform and electrical interface to focus, organize and help standardize these functions for all equipment in every application. The invention can be a stand alone system or a set of interfaced devices or it can be married to any existing system and add to both to create a better set of products and remote control or management and monitoring system.

To the right 600 is the standard cellular phones (Digital (D wave) and analogue) as

the two way transceivers and this circuitry is detailed in the second patent detailing all the modems and cable connections for all the possible C.O.T.S. hand held devices. And also all the PCMCIA cards were described as well as cellular phone IC cards that can be connected to the all the computers listed in the same second patent 112756-200.

601 another two way transceiver option could be any type of radio frequency unit on any frequency and all the frequencies are listed on Figures 9 and 10. The government has a multitude of special application frequencies that might be a requirement for any application specific use, so this is always going to be an option in any PFN for any uses but most especially for high security applications.

602 can be a combination of communication and processor functions integrated consolidated and combined into one system and or a specific C.O.T.S. like the simplified switching device Create-a-link but more sophisticated and capable. Some such products exist presently and were developed for the trucking industry by companies like; LA Guard and Prince, Highway Masters, now part Johnson Controls and the GM Onstar System. And of course these C.O.T.S. products will be easily accommodated and be enhanced in the protected and accountable interface with all the signal security (DES and PGP) in place and required for any high security remote control and or aggressive action. This is another example of a present day versatile application utilizing another technology as part of the protected interface and accountable data storage components of PFN/TRAC. However, all these functions can be provided by the inventions proprietary technology and mini computers if so desired in the proprietary PFN and running TRAC software.

602 also lists the Complete PCMCIA Card which is a product that combines the Cellular phone technology and modem into one device with antenna for lap top computers to function in a wireless environment for phone data connections. This particular C.O.T.S. product has been singled out as one system that will be utilized in the security PFN prototypes and is mentioned here and will be totally detailed in the formal application. Of course in the DES security mode the modem section will have to be modified to accommodate the DES chip set, or this function of encryption will be accomplished in the mini computer which must be able to accommodate the chips and or in the case of PGP encryption run any of the necessary software. TRAC in many cases will provide it's proprietary encrypted software algorithms however, the PFN/TRAC system will be structured to support must all C.O.T.S. software.

The mini computer box directly below, the C.OT.S. transceiver processor option is for the traditional PFN computers either the Basic stamp computers I II or the euro boards 188, 386 and 486 or even those with Pentium processors, that were described in the earlier

patent applicaion (110273-202). The choices of computer processors is once again application specific with the 386 or higher processor being necessary to support full digital video applications with reasonable speed, smoothness, and quality. The other criterion that will give good video quality and properties for the report back function is the on board communication systems, e.g., cellular or wireless phones and any other capable RF transmission equipment on board the host equipment and controlled through the PFN. This system is the shepherd or watch dog to better provide visuals for any of the less capable PFN units that have limited or restricted report back or video quality due to data size, band width, and transmission time capability especially in transmissions from the two way paging system Create-a-Link II (a Motorola Reflex protocol) or as is the case with the one way (pager) receiver as it is configured in Figure 4 which has a total lack of any wireless report back functions in and of itself.

To the right of the mini computer box is the little box GPS number 607 and it is the global positioning system or it can be any type of locating equipment either a separate hand held device interface with cables or as a integrated circuit hardwired into the computer or processor, or merely a chip set as has been described in 112756-202. The last two of which can also be in the form of cards with edge connectors that plug into the euro-board 100 mini computers detailed in the second patent 112756-202 as mentioned above and incorporated herein by reference. One important note is that any and all PFNs can be outfitted with GPS and of course the most sophisticated can provide hot accurate readings and give positions with the military GPS with in centimeters with their additional ground signal that counter the distortion that the ionosphere creates in the commercial versions of the GPS which are within 30 meters as to an accurate location.

So what is the importance of the GPS? It provides accurate geographic audio's and visuals, as well as, environmental telemetry to asses any aggressive personnel, ordinance, and hazards that might be present and in control in a rescue scenario or recovery effort of a lost security area. The pinpoint data reported from the PFNs will provide an important tool to evaluate a hostile situation and determine the best course of action. And as earlier stated the PFN s can help wage an aggressive war, when and if that choice is unavoidable. Or bring a hostile event to an early closure with the least amount of lives lost.

The HPC box to the left of the mini computer box is the Host machines Programmable Computer or control circuit and or processor. This can be the only computer in the secure interface or it can be interfaced with other control circuits or processors either proprietary and or other C.O.T.S. products which are coupled in the secure interface(s) and made a more reliable, accountable monitoring and remote control device termed a PFN which

stands for (protected) Primary Focal Node. The PFN/TRAC system is designed specifically with versatility and universality, to provide a physical platform, with a universal set of electrical connections and interfaces which are ideally standardized as much as possible. And coupled to TRAC authorization and authentication software controlling the local and remote event memory storage functions; to develop a logical organization and manageability for remote control and robotics to meet societies legal requirements and social needs for all the related technologies and their combined functions. This focal point (PFN) and TRAC software on each piece of equipment housing and linking all electrical control circuits with the host peripherals and sensors to off board monitoring and remote controls provide the organization, security and accountability through the TRAC system, to justify to society and meet insurance and security concerns for the use of aggressive remote control and robotics in any scenario. And above all the PFN/TRAC system gives structure to write Standards to: (laws, rules regulations and code) for materials and protocols to perform remote control and robotics by focusing communication, control circuits, data storage and accountable TRAC software in one safe, secure location for the most part. DOD, national security agencies and public governing committees, political bodies and agencies, like; CIA, Secret Service, DOT, highway safety agencies, FAA, FCC, WWW management agencies and organizations, The Justice Department, FBI, law enforcement professional organizations, e.g., IEEE, automotive manufactures and other manufactures, insurance industry, and the many industry standards and watch dog groups, as well as the general public input, should make up the groups that will deliberate and form the laws to be legislated, with the appropriate rules, regulations and protocols needed to plug in much of the appropriate, safe, individually and socially appropriate and legal software commands for TRAC system, as well as, uses for this new technology. The (MMN and WWW) machine messaging network interfaced often with the world wide web and or the Internet from and through the PFN/TRAC gateways created on more and more equipment.

The invention has been expressly designed to help create a responsible organized modality to this emerging area of merging technologies and help to marry it well to societies laws and needs.

To the left of the HPC block there is the host equipment interface which, would be merely an interface connector from the box if the HPC is contained with in the PFN. (These connectors are all shielded and protected in the higher security applications any will enjoy as much protection as is application specifically needed). The lower blocks below 604 is the sensory or telemetry data gathered on the machine and or operator, and the box to the right represents the functional control devices, or the activity control of devices and or accessories

on the host equipment, which will be standard automated controls for the machine and operator for the most part unless there is an application specific need. For example, some of these accessories will be the aggressive defense weapons described earlier and in fact any electrically controlled defense devices can be remotely controlled not only by this sophisticated PFN but even by the simplest PFNs while viewed by this type of PFN or surveillance video cam and controlled remotely. And with these two functions combined any and all equipment operation is achieve through remote control and monitoring all as part of an entire network that give great security options. This provides tremendous back up and force to any security system with constant alternatives to regain control and stability in a threatened security environment with the least risk to all life, which will always be proportionate to the skilled personnel, circumstances and the choices they make.

Returning to the center of the page and specifically the lower center their is three boxes displaying the two levels of on board memory storage with three accompanying numbers 105, 106, 107. These numbers are used to delineate the different types of memory storage devices and not the actual number of devices employed in any specific PFN system. The reason the numbers are used is because these are the present day prototype developments and are listed as present technology, however, due to the vast improvements in memory capacity with all the many different technical variations the invention does not limit its claim to these specific devices and systems that might be employed into this secure PFN interface as the only modalities to establish accountability on board in the PFN.

605 points out that these data storage components and in fact all the PFN devices and components are detailed extensively in the previous patent 112756-202. However the planed universal prototypes in the security area will be detailed presently as to the proprietary devices components and PFN/TRAC system accountability functions. All the prototypes will be completely detailed in this formal patent application 112756-401-and 501

606 is the physical recovery of on board data as has been described thoroughly in Figures 4 and 5 and of course this more sophisticated communication PFN has the off board data storage in the monitoring and control system, which is limitless in the dial up services it can send it encrypted data to. This is not so with the two way pager systems. They must rely on a specific page service provider. And all the two way RF systems are only limited by the amount of transceivers able to receive a signal.

608 is TRAC the programmable and modular software and varies in structure and format based on the different hardware implementations weather it is C.O.T.S. based, PC, Programmable Controller (Stamp); or if it is custom, logic sequencer, micro processor, FPGA (field Programmer Gate Array) or a custom gate array. Even though these are not all

displayed in the three Figures in this application all of these hardware options will probably run some for of TRAC software in some application and therefore should be included as hardware implementations for this technologies PFN/TRAC.

These TRAC Interfaces/Software will have algorithms for BANK/Stock Exchange Transaction Products. Many of these will be supported C.O.T.S. products and through the primary TRAC software. There will be other accountable programs for remotely piloted vehicles RPV and this technologies proprietary PASSS software for the automated slow stop and securing of a vehicle in a stationary position. And this technologies PAGSSS software which has numerous variations but basically it is the proprietary automated guidance slowing stopping and securing of a vehicle through remote control as an evolution of PASSS. Other software specifications include the use of a Commercial:128/64 bit Encryption for web transactions. And for high security in government and military applications: DES the (Data Encrypted Standard)

The interfaces and connectors are named extensively in the related patents however, presently the automobile industry is planning to start a standardization effort for electrical connect-ability of accessories. This technology has been focused on this point or issue in the last two related patent applications and looks forward to participating in any effort to develop H-Rel universal electrical connectors, and can offer actuators, sensor protocols, signal levels in the aggressive automated and remote control devices to reach deeper into a standards effort in this area. This technology will be constructing prototypes with these interfaces anyway and a collaborative effort is always welcome when ever possible. Telephony is another industry interface with Digital Cellular, PCs, 56K modem, pager technology as well as the varied RF signal and light transmission equipment.

These last three Figures have been taken from this technology's security application (110270-400) because these are the hardware components that will support the TRAC software system in the prototypes. This technology has provided the security descriptions in this application to demonstrate the versatility of the PFN/TRAC system and it's uses. No high security strategies or specifics are detailed here and they would be worked out by the appropriate officials and downloaded into the respective PFNs to perform their approved security and defense tasks. The TRAC accountability aspect will serve well to properly use automated and remote controlled force and fairly review that use thereby keep it at the correct level and help to present the truth in any conflict area to aid in any resolution. These PFN/TRAC systems will provide for an organized development of this technology so that it marries well to a democratic and free society that has embarked on the technical road to mass data gathering management and memory storage, while it respects the individuals rights to

privacy by providing accountable protocols for access to personal data. Because PFN/TRAC can provide objective records for all, disputes will become much more clear and easier to resolve. Of course the use and the laws governing any abuse will be determined by the people and their duly elected governing bodies and appropriate government agencies police systems civilly and armed forces globally. Policy would determine by the appropriate levels of governing organization so that any strategic and or defense use deployment and protocols for the PFN/TRAC system with C.O.T.S. products around the world to manage control and or witness altercations and disputes has the correct review and accountability. And this would of course be coupled with world organizations and all involved nations to determine application and use whenever conceivable and possible. These areas would be legislated and laws rules regulations and all the appropriate legal structures would be address and put into place to preserve the best quality of life possible for the individual and their society. The fair deal is possible with this technology but it still requires the people to accomplish it.

Figure 6A

This Figure is devoted to showing the future merging of communication technologies with micro processors and greater memory storage and conversely greater product capabilities and efficiency both in size and function. It has been created deliberately to detail out a good clear commercial evolution of consolidation of technology in the (PFN) so anyone skilled in the arts can easily structure the most cost effective combination of C.O.T.S. products or components to create the best PFN for the present time and into the future. It also has been done to clearly show that all these developments were planned and detailed within the related patent applications to keep the invention current in the future.

6A1 is any and or all telephony technology from land lines to cellular, wireless and or satellite. 6A2 is any and all radio frequency equipment both receiver, transmitters, and or any combination transceivers that are interfaced in and through the PFN. With the continued development and combinations of circuits and devices both 6A1 an 6A will be combined and interfaced as is the case with some phone radio system, e.g., like NEXTEL products and Motorola has other radio and telephony combinations including pager activities. So it is obvious that these will combine into one personalized communication center and that this multi device will be a functional interfaced component in this invention.

The PFN/TRAC/FACT/CEW

For this reason this invention claims the ability to interface and protect and make accountable with all the forms of communication and locating equipment that will also be

interfaced as well as many processor function and the ever increasing memory products available. So 6A1 through 6A4 is for seen as commercial consolidations that will be used in the PFN with more universal circuit use of the same hardware but still all fall with in the nature and scope of the invention because they are all presently individually addressed interfaced and used in the present description of the invention technically and functionally. Continuing on 6A3 is one and two way paging technology of both receivers, transmitters and or transceivers. 6A4 is any locating equipment GPS or combination cell phone and locating function, Lorands or radio fix locating equipment LoJack, etc. In the earlier evolutions these will be separate devices and or parts or components coupled together through hardware which will accommodate both power and control signals to the super modem which is part of the 6A PFN core. This hardware connectable structure is termed the multi-bus Comm Link. It will support a universal plug and play capacity of standard varied connections as has been described in PCT related applications for backward engineering and will also provide digital control signals modulated on the power line by the super modem to the individual devices and components which will be individually addressed by the PFN programming through their individual FACT identity chips and then given the appropriate data ESN/LOT#FCC spec or any other product control and ID data. Then when all components registered by their manufacturer in the National Registry at point of shipment to the commercial market and secondly confirmed when in use in real-time by a legitimate owner and at the point of installation through the PFN and unibus super modem at present completed automatically by the firmware fact chips install by the manufacturer and the FACT software operating in the PFN/TRAC system. This is detailed more extensively in this patent application

6A(UTU) The super modem also supports the unibus internal link in the same manner. This is not per se a new Modem or modem design standard. But the integration in the PFN first level converting circuits to be incorporated and handle application programs from the host machines application specific activity controls and sensors. It will allow for standard connectibles with special adapters and also provide for a control signal which is a modulated digital signal sent out on the power lead to individual activity controls, sensors, operator telemetry and to handle audio and video digital signals.. The super modem 6A(UTU) is a universal transposing unit and will be able to handle analog to digital conversion, digital to analog conversion, all encoding, decoding and encryption processors either in it's firmware or in it's installed software running in the mini-computer section. This modem section can in the future be integrated directly into the communication devices and or combined with the mini-computer section or they might well all be integrated together in hardware and accompanied with the FACT main processor software (that is system or

component failure sensitive with memory storage to confirm functional reliability and emergency power supply and charger circuit as one single protected and sealed protected PFN integrated circuit. If so this is still within the nature and scope of the invention and it's purpose.

Also fiber optics as was detailed in an earlier PCT patent application and may be used to carry control and monitoring signals. In this case the appropriate sensor and converter would be part of the super modem interface and any responsive peripheral circuitry.

In the Multi-Bus Comm Link there will be a universal antenna buss properly shielded grounded and or filtered to provide lower or no noise. Or this universal antenna will be run separately. Ultimately 6A PFN Core will incorporate 6A1 through 6A4 with memory storage 105 through 106 in one self contained protected containment and integrated circuit with a unibus internal interface connector link for any and all past present and future accessories desired. 6A4 and 6A5 illustrate this present interface capability. It should be well understood through this Figure that any consolidation and or combination of communication technology, computing, or controlling processors and memory storage that is used to monitor manage and control man and machine interaction and individual activities from a protected environment and provides accountability falls with in the nature and scope of this invention.

Figure 7

It is important to remember that any structure designed to protect the electronic integrity of any interface and performs the described functions of a PFN as well as, provides protection for any of it's essential peripherals to increase performance, longevity, durability or to increase reliable service, and or to better perform accountable remote control like the TRAC system in any environment all fall within the nature and scope of this invention and all of the above related filings. This is and always has been a major attribute of this technology. To be either universally, and or generally and or specifically constructed for the purpose of protection against any rough service environments and or vandalism or tampering. (The demonstrator prototypes for high security will also have detailed drawings in this formal filing that will basically divide this technology into two product lines of capabilities determined by the type of communication technologies employed. They will be either one or two way transmission capable. However, they may or may not both use the same containment structures. They will once again utilize pager technologies, cellular phone technologies, and or any other RF systems, as well as, light communications either independently or in combination, as has always been maintained throughout all of the related filings.) The only other governing factors will be the requirements of the host equipment, the

desired functions or capabilities, and it's operational environment. It is these considerations that will determine the physical protective characteristics and configuration of any specific PFN.

The other related patents incorporated herein by reference already detail pager and a cell phone PFN s for other commercial industries with less secure requirements. So many of the same innovations and devices will be employed in these high security protocols. Another exception is the detailed described development of greater signal security not just through physical protection of the PFN and peripherals, but also, accompanied by special electrical hardware, firmware and or software TRAC that will handle encrypted conditioned signals generated from a PFN or to a PFN if need be. Also, in this formal application certain other circuits and or electrical components will be specifically designed and or chosen, because they operate well in high electromagnetic fields (EMFs) and or electromagnetic waves (EMW) environments and/or radioactive environments. This will also be the case for many other hazardous or hostile environments (application specific physical and electrical structuring of the PFN).

In Figure 2 only the wall structure is discussed at this time as it will be constructed for specific applications. Ideally the wall will be constructed as a laminated or composite structure for the most cost effective manufacturing, however, in the very specific security applications these wall components might well require specific customization and because of their limited markets increase the cost of a PFN. Ideally universal structures will be standardized in application specific areas to keep cost at a minimum.

700 is the thermal insulating center lamination between two walls, the outer 701 and the inner 702. This center as already detailed in earlier filings and can or will be composed of either fiber glass products, gypsum, silica, mica, asbestos, or asbestos replacement products, Teflon and or high temperature plastics, e.g., polysulphone, all of which would either be adhered to 701 and 702 or merely sandwiched between the two walls. However, one product has been chosen for the experimental prototypes, and it is called "solid smoke" and is a product developed by NASA for the space tile replacement and is completely detailed in earlier application 112756-202.

Due to this center area 700 being a somewhat flexible fill insulation area between generally two solid structures a wire screen mesh, net, grid, or grill of metal properly spaced and constructed from metal products possibly copper, lead, etc., will be placed to block EMF/EMW and or various forms of radiation in special applications. To achieve this additional radiation screen, the mesh can be pressed or impregnated into this insulating composite section in the center of these two walls to add greater protection for the electronic

products housed inside the PFN. This center can and will be designed to provide a soft seal when mated with another section of a PFN wall that will be resistant to the normal elements and harsh chemicals when end sections of 701 are butted up to other 701 end edge sections, e.g., corners (the same for 702) to provide another surface to seal upon, e.g., welding, resins, glues.

Manufacturing can also reduce cost by making three concentric boxes or containers of any application specific PFN shape. One the largest 701 outer wall, 700 the second insulating section and the third and final inner wall box 702. A non flammable glue adhesive or solvent for the insulation section would be applied to the center section and the larger 701 box would have it's inner surface chemically etched or conditioned to receive the pliable adhesive. And the outer surface of box 702 on the smallest box would have its surface prepared in the same way to receive the adhesive (if the surfaces are metal products). The protected cable access hole will be positioned to allow the trapped air to escape upon assembly of all three box sections. This leaves only one side to be installed with mating beveled edges which are both glued and sealed, e.g., welded. This last side or plate will contain the access panel with locking mechanism and hardware (physically and or electrically controlled in most cases). And special consideration is given to any antenna and locking mechanism that is part of this protected containment with hard wiring routed with in the structure (these considerations are application specific with a lot of details in earlier filings).

701 points directly to the outer wall and this wall will be made of hardened metal products (described within) that resists physical penetration as a primary consideration. It also could be coated and or covered on either side, and or even be replaced by a penetration resistant plastic like Culver or other projectile and sharps resistant plastics Teflon, nylon, and, vinyl etc., (especially when the PFN is employed in exposed electrical service application with high current.) This evolution of the outer wall is in keeping with all the earlier designs and claims to provide PFNs to all equipment and environments as continually claimed in all the related patents. However, this exterior wall in some applications will be constructed out of stainless steel and or coated with corrosion resistant coatings or made out of plastic and given special textures or wire webs, grids or grills. That can also help trap EMF\EMW waves and or radiation so as to block their penetration into the electronics housed within the PFN and or any peripherals, if so determined by an application to require this type of protection. Once again any and all of these technical variations can be employed, with the consideration of the tradeoffs. Which are almost certainly to be cost vs. desired and or necessary practical protection.

Through this entire description it is important to remember that any and all of these

protective innovations may be employed, but final products will be constructed application specific and in the most cost effective manner for obvious commercial reasons. An effort will always be made to create the greatest security for the lowest cost, however, the more secure, diverse and specifically sophisticated the unit and system is the greater the cost will be for any single PFN and or the peripheral system.

702 is the inner wall which can and will be constructed of various different materials as already named in the last outer wall description if so determined necessary by application specific criterion for any specific PFN application. It may as well be constructed of hardened steel thermally tempered to increase carbon content in the molecular bonds or a metal alloy composite product may be utilized with, titanium, tungsten depleted uranium etc. (this is the same for all hardened metal applications for the outer wall as well). The inner wall could also be completely constructed of solid lead to create a final protective inner seal against radiation. Or a composite plastic already listed for the 700 and 701 parts with a EMF/EMW wave and radiation screen as already described for 700 and or 701 parts. Once again these could all be used in a laminate of layers or any one could be singled out for application specific priority to control cost. There are also recommended protective handling specifications put out by the federal government and industry for the best modalities to deal with and handle hazardous materials, e.g., radioactive, chemical, bio and medical waste, EMFs, high electrical currents, etc. All the materials used and the manner in which they are used will be developed for the PFN prototype construction with full consideration and compliance with these recommendations and regulations to insure that this technology will be inline with any standard set for any application.

703 shows the thickness of the entire wall, which is once again application specific and will vary as a general rule, but also as a general rule the different PFNS will be designed to be as universal as possible in shape, size and structural composition. The individual walls 701 and 702 may vary in thickness as well as the necessary thickness of insulation. All of these considerations will be application specific. For example in the automobile industry and normal civilian use the protective structuring can be scaled back to a standard that does not require the kind of protections detailed for high security to meet an acceptable standard. This will be true for all applications. They will individually have to be structured to meet the requirements of the application.

704 points out that the PFN will also be structured to be actually part of the host equipment physical structure in some security scenarios and in this case the system would have to be secluded and require limited and or controlled access if it were to have the appropriate military value. It would be structured to assert final control over a piece of

equipment but it's influence would be undetectable and or camouflaged to a large extent and above all extremely difficult to access or terminate. (These systems are reserved for special disclosure and development.)

However, in many cases the PFN will be used to house and protect the host programmable controller (HPC) in the drawings 4-5-6 next to the mini computer contained in the PFN. These functions will ultimately in many cases be integrated with the obvious advantage being consolidation of the vital functional controls of the equipment integrated with partial or the whole data storage, remote control technology with the necessary security components all in one secure spot in a plug and play modular or card form and operated by TRAC software. Which can be physically displaced for an immediate disablement and total securement of a piece of equipment if so desired. But only by authorized and authenticated entry if this is a feature or capability so desired. And Of course any portion of these electrical components can be given this same plug and play capability if so desired.

Figure 7a

This drawing goes on to show in the most general terms how all components can be scaled back in reference to the use and environment of any particular local PFN/TRAC device. These application specific configurations will be determined by standards efforts including NEMA with their already approved containers or boxes for protecting electrical components from explosion and fire from out side. The auto industry and all other industries, e.g., aviation, boating, factory machinery and the military and special governmental agencies use, etc., will all take part in specific design changes or material use to develop application specific containment's for their applications and to meet with the purpose and goal of this technology to preserved and protect the essential local PFN components and memory.

The drawing is explained extensively for extreme environments and the use of double walls may be unnecessary in a great deal of applications. This Figure is self explanatory to most mechanical engineers. The Figure is provided to show the most general and flexible design configurations. And the only other standards effort consideration for protected PFN/TRAC devices is that they be as universal as possible in physical accommodation for all the essential components and accessories.

Figure 8

Displays two variations on the billing box accrediting system and the credit card devices and phone devices that have been innovated for these purposes. Primarily the billing box was designed to be an add on unit or after market device to collect a fee for use of a

vehicle, e.g., rental cars, Taxi Cabs, buses, etc. Part 301 is either a standard credit card, ID card or any other information card that one wishes to use to enter information to the billing box (PFN). However with the price of the smart cards being greatly reduced; this device is not just designed for the regular magnetic strip cards as has been described earlier but is designed to stay current with the more sophisticated cards, as well as evolve to other recognition systems, e.g., finger print and voice and pupil identification systems. Of course the data retrieved from these magnetic cards can be recorded on board in the billing PFN as well as transmitted back to any network gate way that can make the necessary land line connection to any credit check procedure and mass management storage for accounting purposes and records. And when this is done through a billing box or PFN and TRAC system it is a commercial service product of the invention. TRAC can run the bank card/Stock Exchange Transaction products and algorithms via the commercial 128/64 bit Encryption or web transaction. And or utilize the C.O.T.S. banking products and protocols, These will be named and given more detail in the formal application. These transactions will be provided memory storage for personal accounting and verification to the financial institutions as proof of payment. PFNs will be every where and all those with ID systems PIN number and key pads, finger prints and other forms of personal identifications will allow for the personal payment virtually anywhere.

Part 802 is the regular or standard cell phone handset that if it is in use the lower bill box could be configured with out a key pad. Part 803 is a standard key pad format that can be used to communicate with the bill box when connected and interfaced with any the invention's computer and supported with the proper interfaces and software and or firm ware. Part 804 is a multibus bar connector universal with 29 contacts so that it can support any system/device entered into the bill box. These were earlier designs. And this earlier design will probably not be used and will be replace by the multi bus system IEEE1394 or the universal bus and or IrDA interface.

Part 805 is a quick connect end on one portion that will make a pigtail to connect with any combination of electrical connectors on the other end of this second portion, e.g., computers, any electronic connections, radio or automobile, but in this case is depicted in the drawing as RS232 part number 806. The other short pigtail is part number 805, there may be 5 to 10 in quantity, that can slide easily back and forth to allow many varied positions for the different devices and the space they require. All hardwired connections could be made with Commercial Off the Shelf devices in the box or by infrared com port connections. A segmented infrared bar can be aligned to any device's infrared window to communicate with the invention's control circuits. Also there are varied but designated power connections to

supply power to any device by priority. Once again most all devices presently will be configured to IEEE1394 USB connections and have the drivers and software supplied by the manufactures to quickly install almost any desired system as easy as buying a product peripheral for a personal computer. This is one of the main reasons for the timely presentation of the invention.

After the devices are installed and connected, foam pad shims are placed between the different devices to quickly secure them in a protected stationary position. The dotted lines show adjustable bin space for the user to plan their own devices. Part 807 is a mouse ball that one can use to run window type graphic programs either displayed in the unit display 808 and/or any larger display within the field of view for the driver, either LCD vacuum tubes, e.g., VGA flat screen, or the new hologram wind screen in the newer cars (e.g., Pontiac Grand Prix). Part 808 is the unit display, part 809 is an emergency power pack, and part 810 is the secure bill box.

The structure of the box has been described in the best mode of carrying out the invention as to it's wall structure and insulated characteristics and will be modified and or configured in many different shapes and sizes if necessary, however an attempt to standardize all boxes in their categories will be a main consideration in the commercial development of the invention.

Figure 9

Is a Figure from the original patent an it illustrates a one way pager PFN/TRAC containment with it's protective encasement because there is a need for many cost effective receiving devices for the MMN. This one way pager system was created to perform the proprietary vehicle shutdown PASS as a cost effective modality to be added on to cars to aid law enforcement end high speed chases. However this system can be used to remotely control in an accountable manner a piece of equipment when connected up to the appropriate activity controls that either interface electrically or perform push/pull and or rotational operations to control virtually every piece of equipment through automated and remote control.

901 is a manual lock for the PFN and these can be at any quality desired. It also has an electrical connection to be use in arming the device. 902 is the memory storage in this case audio recordings and a flash memory of operational data (Sony's memory stick 8 meg a bites a piece). 903 is using a stamp processor as the controller. 905 is employing OCR systems however Motorola has many C.O.T.S. products that can hook up with direct connections and all are covered in the related patents. In fact this entire system has been well detailed in all the related patent applications.

Figure 10

Shows a picture of a dash board in a traditional sedan. Just right of the dash is the PFN and it is depicted as a box with a personal computer slid all the way out of the containment with the lid or screen display opened so that the driver could use the computer screen with a GPS system like DeLorme running to receive automated directions to an address he was unfamiliar with. Below the computer and the secure lock up center section rests a cellular phone that has its phone modem connector coupled to the heal of the phone and directly to the right is a second communication device a pager that is also coupled to an optical scanner in this case as was described in the first patent. The lock up 1004 in the center can house permanent invention computers and storage records plus GPS and any communication devices that are desired on the vehicle all the time, This lock up section is only accessible by authorized personnel in the most ideal situation and hopefully mandated by law. This section would house the PFN invention computers and in the place of an on board personal computer their would be an LCD screen that could display map graphics if need be, through the on board computer systems.

This is only one basic configuration for a PFN and the system could be re arranged in any number of ways.

Now for a more specific parts description of the individual parts numbered. The square boarder with circles inside is the walls of the PFN case. 1001 is the outer metal case plate which can be up to 3/16" thick made out of AR metal plate to resist penetration or drilling. 1002 is the inner metal plate up to a 1/8" thick and it is made of the same AR plate. 1003 is an insulating product and their is two that are being used to construct the prototypes. One is "solid smoke" a product developed for the space shuttle and "Geo-bond" a gypsum product. None of these products or specifications should be considered the only way to create a secure PFN containment to fulfill any part of the nature and scope of this invention. The thickness of 1003 the insulating section would not exceed 3/8". 1004 represents one kind of lock cylinder like those used in safety deposit boxes, however, not made of a soft metal like brass. From 1004 can be seen two flat bars that go out past the inner plate 1002 where they pass through a solenoid catch mechanism that when it is de-energized will not allow the bars to pass out of the front edge of the encasement. 1004 in the center can also be opened manually with a key. Once again there are many manual and or electrically automated locking devices that could be utilized for this same purpose.

In Figure 10, 1004 is displaying the bottom compartments access panel swung open on a piano hinge part number 1006. So the view is displaying the back of the panel so bars can be seen and that is why they are depicted as solid lines. Behind 1004 lies the secured

section which is represented with dotted circles because they are located in back of the bottom access panel in the open position. If the center section is the designated section to handle or store the legal storage electrical components it will not have an electric lock release or it will be disconnected to only allow for the proper authorities to remove this data or component parts. 1005 is the bottom access door in the closed position and that is why the bars are depicted in dotted lines. Once again 1006 is a piano hinge and is a part on each of the three sections as a point of articulation for the panel door. 1007 is the standard glove box that can either be used or discontinued to allow for other rerouted accessories HVAC vent, ducting and planums or blowers motors, etc. 1008 is the SIR compartment which is the sudden impact restraint or the Air bag. With on board distance sensing for front and rear as well as even side surveillance of the environment any impending impact would be sensed and automatically with draw any opened draws in use into the containment which would allow the aesthetic skin panel/drink holding table to spring return to a closed position. If the drinks were in the table with the table in the down position all 3 access panel doors would be closed and secured. This would be accomplished by electric servo motors or vacuum motors or cylinders or diaphragm systems for speed. Also the electric cylinders could be used, e.g., "Memory metal cylinders." At no time would the center section or a part of the center section be open to the cabin during operation as this is the protected black box storage area. Of course these configurations are flexible and the designs can very greatly, but when a permanent area is chosen it has to remain inaccessible till the proper authorized personnel supervise any reconfiguration, e.g., certified service personnel that have to enter their service identity credentials. Otherwise a customers insurance company must do the same or support clerical personnel for the police or department of motor vehicles.

1010 is the pager as earlier described with a scanner on the front however any interface and connector system could be employed in the PFN. Also Motorola pager processor "Create-a-Link could be utilized here and even as an effective processor in the center section that is closed for the ultimate secure service functions as another C.O.T.S. computer communication combination for the inventions control center. 1011 is the standard cell phone with 409 depicting a connector modem, which will be wired through the trays to any on board computer to receive and transmit data to any system in the PFN or connected to it. 1012 is a specialized tray connector made by or for the personal laptop computer that will provide all or any of the desired physical connections to interface the computer to the host vehicle or any other peripherals or to net work it with any other computers. The holding and securing tray will then couple to the sliding either motorized or powered by vacuum. And so the electrical connections to be functional here it will have a controlled flex cable to 1103 the

central buss channel or canaleta or race way where it will route wiring up and down inside the containment.

Figure 11

Figure 11 shows two views of the secure box for the PFN in the Dash. The top view is of the back of the box cut off so the components can be viewed. The top shelf is showing a laptop with all its varied connections that have a performed shelf designed to supply the necessary connections directly to the laptop connectors. There also is a tube or channel part 1103 running from top to bottom in the back of the case in which all the shelf connecting leads are channeled together and all the appropriate connections have been secured to the devices in their shelved trays. This same tube works as an antenna galley and channel to house the control buss of wires to the out side of the secured and protected PFN. These wires are protected in a armored flex cable like the one described in the first patent for the protected beeper.

When 1103 doubles also as a antenna galley in the back of the PFN and for the full height of the containment the outer metal plate part 1101 is replaced with a strip of Amoco's poly-sulfone thermal plastic ½" thick 1 and 1\2" wide strip which runs the height of the box some 9 to 10 inches long. This thermal window is provided in the back of the PFN to make it very difficult for anyone to tamper with these vital circuits and to also allow for a signal to be received when the C.O.T.S. products patch antennas are not sufficient and they have provided for an external antenna hook up. And as also mentioned earlier there is another option to provide for reception in the protected containment to receive any necessary signals through using the same poly-sulfone product and creating port holes for the necessary signals to enter into the protected containment to reach the standard C.O.T.S. antennas, e.g.,patch type, but also provide protection from heat and fire. And of course these port holes would be located in hard to reach areas.

The bottom box illustrated in Figure 11 is showing the lock access panel doors with a piano hinge 1106 for this sturdy structure.This 1/8" thick access door is made out of stainless steel and numbered 1110 in Figure 11. As mentioned earlier along with adding an additional way, the access doors 1110 can be opened in three different ways, one with a key in two places as displayed in Figure 11, another as described in Figure 10 with the throw bars out to the electric solenoid catch mechanisms and there by finally opened by electric solenoid release triggered from the inside program software of the inventions on board controllers which is reliably energized by the emergency batteries inside the PFN. The two key system would also have the same solenoid lock release system.

These access doors and locks are finally covered by an upholstered and padded dash plate/drink holding table numbered 1107 which is illustrated in the down and open position and appears as the end view of this dash plate/drink table. The front is molded and formed to create a uniform appearance to the dash board. This aesthetic dash front may be constructed by covering the compartment panels with cushioning and upholstery and not having the drink top dash panel.

However, 1101 represents a molded rubber gasket that is grooved to accept the dash plate/drink table in the closed position. 1102 is the two sided lock placement cylinders if this type of lock system is employed. And 1111 depicts the electric latch plate and solenoid assembly that receives the lock bolts from the keyed cylinders. 1105 is another piano swing hinge for the table/dash cover plate. 1104 is a coiled spring that returns the dash plate when all the drawers and/or trays are retracted. 1106 is a shelf roller that can be slid into any number of slots in many places of 1002 the inner wall of the box. These slots will either accept a tee ended fastener that supports these shelf casters or rollers or it will allow a compartment plate or separating partition wall to be slid down the slot. These compartment shelves or rollers can be moved or exchanged to create any number of configurations, however, the trays will be standardized to certain sizes that will be customized by the manufactures to accommodate their products.

These separating plates have lock blocks that have drillings with 10/32" screws that will thread into tapped receiving holes in 1002 the inner wall. 1108 in one of these partitions. 1106 the rollers have a screw that can be tightened to clamp the tee device against the inner wall skin- part 1002. 1012 is the personal lap top in the top shelf. 1109 is the trays that ride on the rollers. these trays presently are designed to either be half the size of the PFN or to go all the way across the containment. This is not the only design for the movable trays and adjustable flat compartments and should not be considered so, but this design is being prototyped presently. Any protected containment or interface that is structured to coordinate and control remote functions on a machine all fall within the nature and scope of the invention.

Figure 12

Depicts 3 possible drawers configurations for a possible application of the secure box and the PFN equipment. The top draw houses the laptop computer 1012, the bottom draw houses the power pack batteries 1201 and 1202, the transformer 1213 and the inverter 1203 along with power supplies that are varied power taps 1217 for the C.O.T.S. products housed in the PFN. And the center drawer houses all the essentials to complete the necessary

function for the PFN. It has a GPS 1216, A Cell Phone 1205 a Pager 1209 and a small PFN computer or controller 1211 and a data storage MO or rewritable CD's disk drive or hard drives or memory sticks 1212. With the drawers and compartments 12.5 x 12.5 x3" all components easily fit into the three drawers.

The top drawer 1214 is showing the multiple fittings that would be molded into the tray and not visible as a end view but instead as a top or side view. In most cases the manufacture would not have to outfit a tray and probably would not do so for all the possible connections for the laptop. However they are shown here and mentioned as all being possible. Reading from left to right the first connection would be for 14.vdc as a power input for the computer and is supplied by the bottom shelf tray from part 1214. On the top shelf again the next round circle to the right of the DC power connector icon the PS2 mouse or keyboard connection for an external mouse or GPS 1216 connection in some cases. The next comport is a 9 pin serial port and the following one is a 9 hole additional monitor port. Then the little square is the infrared communication port, and the very next one is a parallel printer port 25 hole LPT1 port and the last one on the left is the a USB communication port and most likely the one that will be used with any peripheral hook ups in the box, however any of these connections might be used for any number of interface connections and it is possible that a laptop manufacture or secondary provider for the trays may outfit any and or all the communication ports with a service connector in the tray. Ideally the placement into the tray or cartridge that is affixed to the rollers and rolls it self or is placed on a shelf and does so. In any case the tray or cartridge for any peripheral will instantly plug up to the laptop or other device when placed and secured in it. This would replace any need for thumb screws to complete any required secured connecting unions. And would accomplish a plug and play modality for rapid deployment into a PFN's electronic array of accessories as a compliment to the full complement of the inventions electronic devices and innovations. These have been detailed earlier and their exact configuration will depend on how much the OEM of the host machine will provide in their PCM or accessories. But as was illustrated earlier the components to provide all the stated services are available through the inventions technology if need be.

The bottom shelf or power tray as designed for this prototype will have two batteries one a 12vdc part number 1202 and a 6vdc part no. 1201 and these two batteries are wired in series to create 18 volts, which is wired into the primary windings of the transformer 1213 that provides multiple current level taps or solid state regulated chip circuits to energize all the varied C.O.T.S. products in the PFN. These prototype voltages are 1.5 vdc, 3.vdc, 6 vdc, 7.5 vdc, 12 vdc, 14.5 vdc. 18-19.5 vdc and also because in many cases people will enjoy

being able to plug their computers right in 1204 is provided as a transformer and rectifier or converter and tied directly to the primary coil of the transformer 1213, 1204 receives it's power from a 120 vac circuit that is created from the host vehicles 12vdc supply of 6 amps and the PFN battery pack energizing an inverter of 250 watts, which also supplies 120vac to a plug prt.#1217 in the front stainless steel access plate for other devices that people might need 120 volts AC. , e.g., small heating blanket, coffee pot and/or hair dryer

In the second draw 1207,1208,1217 are OCR optical character recognition scanning devices and they are wired to a micro processor so that the unique digital signal from a scanned alpha-numeric image on any and all of the devices that have LCD displays, e.g., GPS, cellphone, pager and respond to any appropriately addressed message with the proper preprogrammed response as described in the first application.

This scanning interface is only one example most all the of these C.O.T.S. devices have their own interfaces to allow them to communicate with any onboard computer they are connected to, e.g., serial or TTL, etc. And any of the IC components would be all part of a circuit if it was in the secure lock up as a mandated circuit function by law. 1206 is a connector for a cellular phone. and on the back of the tray are a number of different sockets for data transfer cables to the 503 wire race or cable channel that goes from top to bottom in the containment.

In the back of the middle drawer part number 1215 indicate a lock partition wall in this prototype and behind this wall is where the PFN controller/computer 1211 is along with its' data storage system 1212

The hardware connectable are detailed for present technology in the earlier related patents and there has been an on going effort to provide forward and backward engineering as well a construct many modalities as prototypes for the PFN/TRAC system

Figure 13

This is a self-explanatory chart and universal PFN to show the accountable data storage for on board a well as the remote communication services that can be referred to when reading and viewing Figures 3-4-5, 6 and 6A with all the different types of communications detailed. The chart and universal PFN will quickly provide a basic understanding of the report back properties and remote data storage systems to expect form an individual PFN and any communication service it is employing.

Figure 13 is an interior block diagram as to how a card swipe or card swipe cell phone would be connected to one of the billing box or PFN computers and would then process the magnetic data stored on a card through the software provided by the card swipe

manufacturers, as well as any credit card company proprietary security software used by the PFN computer. An electronic signal with a preprogrammed dial up number to a credit card approval service company with any proprietary software to process the data in the remote location would be partially and or either held on the card or in the PFN software package depending on the type of cards and devices chosen to complete this remote billing and payment procedure, e.g., smart cards vs. regular cards, etc.

This data because, in most cases will require a radio transmission should be sent as an encrypted algorithm to protect against any criminal hackers pirating legitimate credit card information out of the airways. Most credit card strip reader manufacturers design them to meet standards and protocols such as ISO 7811, 7811/1~6 and or comply with DMV format for driver licenses. They are also all CE, FCC, UL, CUL certified. These devices were all discussed earlier in the devices that could be interfaced with the PFN's as peripherals section of this application to provide mobile remote services.

It is important to understand this mobile paying function of the billing box currently shown in Figure 8 as a add on devices for cabs, limo's, automated rental equipment and vehicles, etc. is only the after market version of the PFN's total function to provide a means to pay for equipment use and any and all services surrounding vehicle and equipment use commercially. This card swipe is another peripheral that will be on all manufacture vehicles in time as part of any PFN's to allow for a vehicle \ equipment operator to pay for any use fees, uncontested tickets, or to log driver license information, and or pay energy fees immediately, rather than having to stop the vehicle to stay current monetarily for use of the vehicle or services. They can card swipe at any time, either while taking on any energy provisions or at any convenient time in the comfort of their vehicle out of the elements while using the equipment/vehicle simultaneously.

As was mentioned earlier personal identification equipment e.g., fingerprinting, papillary ID, voice recognition, pin number from key\number pad, ID transmission bracelets, etc used as either additional ID conformation peripheral systems or a future primary personal ID credit device component to a remote or PFN personal credit data storage accounting system will be connected and interfaced in the same manner as illustrated in Figure 13a. Or these systems will employ any of the interface technology shown in Figure 7. In the case of the transmission bracelets of course the on board PFN universal RF receiver section will receive the signal and have a serial data conditioning of the signal encoder or this will be a function of the PFN computer processor and software through a special IC decoder\encoder card part of the computer hardware.

Also for security the transmitted data will be recorded in the PFN memory systems

e.g., hard drives, buffers or flash memory devices or MO drives or CD write drives, etc. as well as any remote location credit data management and storage system. Accompanying the credit data and amount request will be the ESNVIN number of the sending PFN along with time date and locator coordinates for the billing, charging, ticketing and acceptance of as well as any acceptance criterion for these transactions, e.g., electronic signature or hard copies generated by on board printers etc. which are turned in with a transfer of memory at the end of a shift or use of a vehicle or service.

In drawing 13, 1302 is a cell phone that can either be inside the billing box or outside and only electronically connected. 1302 here is out fitted with a card swipe slot that can read the magnet IC strip of a credit card or a driver ID, etc. There are two electrical connection shown coming from the special cell phone 1320 and 1321. 1320 goes to a PCMCIA modem to support data communication by a cellular phone for the PFN computer. These actual connectors can be serial RS232 connections or IC cards configured into the PFN computer hardware mother board, euroboard or done with edge ribbon connectors etc. 1321 illustrates a direct connection if the special cellular phone is already out fitted for data delivery in its circuitry and therefore would connect directly with the computers RS232 with a mere cable or utilize the new 1394 universal bus system or utilize any connection to handle TTL or the standard serial port PS2. For this multi tasking phone to both send and receive data through the cellular system and to process the digital data retrieved from the magnetic strip a function switch will send a firmware stored signal to the PFN to process and store the card swipe data in it's hard drive if on board or in it's processor buffer to be retrieved and sent via the PCMCIA modem to the cell phone and to the remote location. As stated earlier this function could be manually contrived with the button first processing and then in another position sending it as data through the cellular protocol. Or this data could be performed through soft ware commands stored on the card and PFN or even in the cell phones firmware, e.g., D-WAVE phone protocol from Sony and its multitasking capability out fitted with a card swipe. 1301 is a plain card swipe possibly one of the ACETEK series mentioned earlier as this invention's experimental prototype products. It connects directly to the PFN computer either serial PS2, RS232, or simple transistor to transistor logic TTL. 1306a merely depicts these interface options as well as shows the special cellular phone could supply its card data in this manner in one modality. 1311 is a PFN computer and is one ideally with at least a 386 processor as was described in the processor and computer section of the PFN's described earlier. 1311 would also be programmed with all the necessary and proprietary software to complete these security billing procedures. In the lower left corner of 1311 is a small square with the letter [B] this stands for buffer or hard drive in the PFN computer.

The number 1319 has lines that go to the little square [B] on 1311 and to the horizontal square to the left. The horizontal memory square is additional memory to keep a record of credit tans action most probably done with Sony memory sticks, how ever any of the memory systems described could be utilized and then erased by the proper procedures after any reasonable tie had past on questionable charge entries.

1323 with a lighting symbol signifies a wireless cellular signal conditioning device for data transmission to and from PC's. [PCMCIA] in a square. 1313 is a two way data modulator for any RF transmitters, receivers, or transmitters, used to down load data from the PFN or in this case the card swipe protocol to a remote location or gateway, etc. 1314 is a two way Motorola reflex protocol to down load data to a remote location. This would involve PFN software that could break up the data into 20 bit segments and transmit the data to a remote location that could reconstitute any lengthy multiple transmission into a complete secure text transmission if it is determined necessary to develop a secure algorithmic protocol for credit card data transfers. However, Motorola is very protective of these transmission signal protocols already and this might prove a secure system if practically capable of handling the quantity of data in any commercial transaction.

All these different data communication pathways are being discussed presently for the use of the card swipe billing to demonstrate the connectability of all the previously described peripherals and to demonstrate to anyone skilled in the art the ease, feasibility, practicality and obvious reasonable development of this inventions interfaces to organize and control the process to combine all types of communication, e.g., wireless, and land based, into a protected focal center that is capable of processing and controlling, recording reporting and billing for the use of equipment and related services in an accountable modality or protocol.

1322 is a new product that adds so much to ease interfacing of cellular technology to the PFN and that is why it is mentioned here directly. It is a complete data hook up of modem transceiver and antenna with a PCMCIA III connectability to any of the PFN computers. The last square is a standard telephone data modem for computer data transfer, the little circled (H) stands for hard wired to land phone lines; and is listed hear to demonstrate that the PFN will be used with stationary equipment as well as mobile equipment and vehicles to value use and service related to use as well. 1318 shows the connectability of all these data conditioning and transmission devices described above and in Figure 7 and within this application and all related applications. 1318 also shows that the memory 1319 will store any crucial down loaded data to a remote location on board the PFN as well.

1315 is a pager receiving station, 1316 is a cellular phone receiving station, and 1317 is a radio frequency station and these are all wireless to land based phone node systems, they

can be gateways or they can provide wireless communication through standard ISDN phone lines to secondary commercial, private or public entities that perform gateway functions, accounting services and or monitoring and or remote control function to a vehicle\equipment or any multitude of net work services as shown for all three wireless communication modalities in drawing 13. However, one important note to remember is that the listing of these commercial, governmental public and or private functions and services listed in Figure 13 under each of these wireless modalities is in no way confining to a specific wireless modality. These services could function in any one of these wireless modalities and, in fact, use a multitude of them. Some of the services named here do not relate solely to the car swipe system functions either. Drawing 13 demonstrates and drawing 3 explain how all the peripherals are to be interfaced and the functions named for the three wireless modalities serve only as a space to reiterate all these vast functions that the PFN will be capable of though all it's networked devices. This entire document and related applications detail all the peripherals and their interfaces which fall within the claims of this invention. And the mere fact that some service is not mentioned by name in this application or any of the related application does it mean that it is excluded from the claims which make up the nature and scope claim of accountability as it relates to any vehicle/equipment use, abuse, unauthorized use and or any related services provided for any use or in equating any abuse or damage of a vehicle or piece of equipment, person or property.

Figure 13A

This Figure is a similar Figure to 13 but is included here because it comes from another related PFN application and it shows some of the consolidation of devices and components in a universal PFN. This is continually done through out the PFN applications to provide flexibility in constructing PFNS out of existing technologies and to establish a mutual organizational platform to perform accountable local interfacing. The progressive consolidation of these devices, components and modalities are well documented in PFN applications and all fall within the nature and scope of the invention. They are meant to be inclusive in the specifications and in the claims of the PFN invention. This was done deliberately to draw all manufactures into a cooperative effort to organize and standardize an accountable interface platform and system for machine messaging robotics and remote control and management. So basically these variations and modalities are offered to aid anyone skilled in the arts to have all the options and versatility to interface there devices and product with the PFN/TRAC System. It is a major objective of the PFN/ technology to be inclusive not exclusive and to perpetuate equitable sharing of knowledge data and cooperation to

increase markets, products and services for the public and the economy through beneficial commercial ventures.

So this Figure depicts a universal PFN system with some usual device applications and varied hardware hook ups to communicate with the remote locations and physically perform the Accountable Remote and Automated Control for society and it's institutions. The bold black line with universal PFN enclosed is to indicate that this is a protected area not just physically but legally. In the enclosure 13a1 is a commercial off the shelf C.O.T.S. cellular phone it show one modality of connectable hardware through a PCMCIA modem connection 13a2 to the processor and internal TRAC\FACT software (these connections are detailed as standard hardware connections in all the related PFN patent applications or one of the new PFN uni-buss type connections. In this application all the software is commercial off the shelf supplied by the cellular phone company and or the PCMCIA modem card interface (presently a windows based programming for local plug, program and play capability to enter preprogrammed commands via PFN keypad, display or serial input (software commands are application specific by governmental and industry protocols and geographic area -determined by standards efforts) rules regulations or laws. Obviously this preprogrammed software would be down loaded and the appropriate dial out phone numbers installed in the command string all as a software download or entered by authorized individual with proper PIN codes, and appropriate application specific security codes. This of course can be accomplished remotely from intranet and Internet access and interfacing. This would be done through commercial servers and or public providers as illustrated by the little men at their computer terminals feeding 300C national government, and 300 L for local government as part of the whole 300 networking system serving the PFN communication system including IP gateways for RF, Paging systems and or wireless telephony. These are shown to have land line ISDN, fiber optic, microwave, with all necessary phone routing system to provide the service on an intranet or Internet with any level of security applications determined by the authorities.

However, even these commercial servers, would have emergency protocols and system programming to meet any standards effort regulation to operate as part of the system. As detailed earlier these mass data handling gateways and storage systems either commercial servers, or publicly provided will have to meet ongoing inspections to be licensed and operate in the system. Their involvement in the PFN/TRAC system will be governed by their real-time service capability and their charging rate can be automated to reflect their availability an actual performance to serve. Also, automated routing will provide uninterrupted service or other possibilities to compromised systems during a state of emergency and provide tracking records in all the local memory storage systems both in the PFNS and the TRAC Systems

mass data handling, management and memory storage units. This accountability is provided to understand any failures and assess any blame or liability for society, the individual and societies institutions to react to and correct.

Below the PCMCIA connection block is the block called Complete Card. This is a desired modality for cellular phone use in the invention. It employs a commercial off the shelf C.O.T.S. product a PCMCIA Complete Card ™. The complete card also supplies its own software and hooks up in the same manner as a PCMCIA standard modem card. However this system also incorporates the Cellular phone system and antenna. The appropriate hardware is known in the industry and the appropriate configurations can be accomplished by anyone skilled in the art to link up the euro100 boards with the PCMCIA connections. The bottom box is modem and can be part of the top box PCMCIA connection when used with telephony or with any application from the lower box 13a8.

Number 13a8 box shows all the different types of communication devices employed in the PFN's. 1 way Radio, 2way radio.1 way paging, 2way paging, light or sound and GPS or locating systems. These different communication devices are well covered in the in Figures 3,4,5, and 6 and will not be revisited at this time. However, as this drawing illustrates they would process their data streams through the modem and on into the processor to be handled by the TRAC/ FACT/CEW programs etc. The modem would be capable of converting the applicable data steam and communication source to be used by the PFN processors. In this same block light and sound as well as any other electromagnetic wave that can be used to transmit wireless or hard wired to a converter or modem to deliver control signals to the PFN system are hereby included by reference as another modality of communication.

The modem box also ha a small (S) in the of the box to represent super modem. In the consolidation of I.C. components for processing signals data pathways are shown from the system under control (the open dots) as well as all forms of communications wired and wireless entering the super modem via the unibus caring all forms of signals that will be processed for one input connectable. The PFN processor/computer with memory and modem will then be further consolidated into one device as small as a present day cellular phone. However, this personal PFN communication device well detailed I all related PFN applications will be in many personal item forms with a variety of configurations and applications (belts collars, purses, briefcases palmtops. But they will all be multitasking accountable communication arrays. Device with a host of accessories or connectables to perform accountable tracking and remote and automated control functions. These same reduction in size consolidation and integration of circuits and devices increase the capability

procedures and will also be utilized in the equipment PFNS as is detailed in the related application and is inherent to the PFNS nature and scope.

In earlier related patent applications traffic control devices were described for authorized personnel to control in real-time a particular vehicle by pointing such a tool to a specific target vehicles receiving plate and to control a slow guide stop and secure sequence for a suspect vehicle.

13a7 is the uni–Buss connector that has also been discussed earlier. However, ideally an accepted industry standard will provide a universal plug, program and play capability and the TRAC/FACT software and TRACS management system will insure accountability and real-time control as needed. All possible present connectable hardware was detailed in the related application docket No. 112756-202. However, as stated before the plug, program and play capability for power sensing and control signals is part of this technology as described in Figure 6a as natural evolution of this invention. Whether it is for a mobile application (car) and or a stationary devices or personal PFN devices the control power and signals to the processor can basically use the same kind of plug program and play Buss connectable system. 13a3 is the mini-computer containing the TRAC/FACT programs. The round circle is for the CEW program Commercial Encryption on the WEB. This software program is provided by the credit card companies and will have a special modem capability and handle 128/64 bit (presently and of course as more improved software protocols are developed the system and hardware will be altered to accept any new standard all with in the nature and scope of the PFN/TRAC system and invention.13a4 is a card swipe or reader that is connected to the processor either through the uni-buss or the old R232,TTL, or PS2 type of connections. These three are shown here as the present standard connectable set of modalities known to the present industry but are not limiting for the PFN/TRAC invention. However the un-Buss connector would be a more ideal modality for space greater data flow, and efficiency. These old standard connections are shown to be available to other components interfaced in the PFN and can be employed to give forward and backward engineering versatility. These would be limited in number as time went on and would have separate software commands and programming, with the appropriate drivers to access the different Com. Ports (Serial, USB, IRDA, Parallel, ect) and coupled device to complete the interface with the PFN. The device would still have to have an electronic FACT ESN or identity system or would require special registration to be interfaced. 13a4 the credit card reader would be able to handle commercial credit cards and driver licenses and FACT SYSTEM identity cards.

13a5 is the hard drive on going memory storage. For size reasons in this drawing the FACT applications specific event memory is not shown, but it is a redundant memory to the

continuing running memory on the hard drive (or preferred memory storage as many modalities for memory storage in the PFNS are detailed throughout all the related PFN applications. The event recordings are controlled either automatically by resident PFN programs, or remotely activated and controlled by an authorized external source (Logged command string) or by the resident operator or occupant. In any event all machine and man actions and interactions are recorded and logged in the FACT Memory preserved in the protected restricted access area as depicted and detailed in Figure 7,8,9,10 and 11.

13a9 is a big dotted line, which is the uni-Buss going out of the PFN and going to activity controls video cameras (or Digital) microphones and activity sensors as well as generic host control connections or SUC System Under Control. Some of these sensitive control and sensor leads will be provided PFN protection special and or utilize the host vehicles strongest architectural structure (e.g. the frame) to protect these critical transmission lines. This should be determined application specific and as part of a standards effort. I have gone though a great deal of effort to detail all the properties and qualities and give modality examples to provide a standards effort a good clear organizational system structure and electrical interface platform to provide Accountable aggressive remote and automated control for society and it's institutions. However before leaving the local universal PFN structure is an important point of accountability and fail safe protections is a self enclosed power source 13a10, which has bee a part of the PFN systems from the outset including the Stop and control box. Of course the emergency power system is charge maintained from a host piece of equipment or some other alternative source (solar Cells, land line, mechanical, or chemical, etc.) depending on the application and type of PFN). But it is protected in the protected encasement and capable of supplying power to the essential operations or control systems as needed or necessary functions. The TRAC system can fail and there is no fail safe that can prevent all failures or tampering attempts, however as part of the PFN/TRAC component system is that each element can report it's last correct operating time, and data inputs, so that a record is made of the components time of malfunction and un-reliable operation for accountability and accurate use can be determined and assessed.

300C in Figure 13a is the commercial server, who can be any gateway node the customer picks or can be a service provider for the OEM host equipment or an energy provider or a bank card provider or a communication company or any type or number of these commercial servers. However they must be licensed and provide enough mass storage to handle all critical TRACS/FACT data to operate in any geographic area. They also have to be able to handle it in a secure accountable manner. For simplicity purposes the 300C have been placed at the bottom of the 3 basic different types of present wireless communication. To the

right cellular phone system, to the lower left of Figure 19 is the present one and two way paging systems and for the lower right is the Radio frequency systems. All of these systems connected to land lines (fiber-optics, ISDN, etc.) to perform any hardwired Database connections they are computer operated and act ac gateways to isolated computer networks and can provide web access on the Internet. (if need be encrypted). A sample of the types of commercial businesses that would utilize each type of communication technology has been listed under their respective areas. This is in no way intended to represent all the possible commercial uses as the PFN will ultimately be on every piece of equipment.

In the middle right the rest of the 300 system is illustrated by the large computer stations manned. The one with L.G.A.&C. SYS. Stands for Local Government, Access & Control System. And the one labeled N.G.A.& C. SYS. Stands for National Government Access & Control System. In all communication areas and in the extreme lower right hand corner is satellite and a satellite dish connected to land base phone lines. This is to show that the national registry can provide complete critical TRACS control and FACT data to it's entire geographic area and is also capable of transferring Data internationally at the proper authorities desecration. Some of the proper government agencies are also listed but all government agencies could access and create data as could even the general citizenry for total accountability. of course specific data on individuals would not be obtainable or used unless authorized by the individual or as the result of some legal action as is the present case. Any such misuse or access would be reported to the individual and alert the authorities and the person violating a persons individual privacy would be criminally charged and subject to civil action as would any agency or commercial storage area. This means total accountability. This system has been designed to respect individual privacy. Which means that the individual has to release any licensed storage facility public or private no mater if they provide the service free of charge or not. However, Gross non descriptive data can be sold and discriminated as long as an individual can not be identified or compromised in life the pocket and the pursuit of happiness. The exceptions to this rule is that if through the course of operation a piece of machinery they endanger others (public Safety) then the proper authorities and commercial insurance agencies can access these personal records. However an individual can give permission electronically in real-time if so desired with a signature of a PIN number for consent or a verbal voice recognition or the fingerprint steering wheel, video snap shot, or a signature on an electronic pad or the iris reader and voice recognition or any combination of the above. Free service can be provided and personal data can be acquired and used if this is agreeable to the individual.

Figure 14

Along with many other secure sealing mechanisms this technology provides an additional security feature for the PFN secure on board memory, as well as, any other necessary electronic parts. The electronic certified seal system: Figure 14 is utilizing one thousand series numbers on this drawing because it uses the coyote relay systems (from an earlier filing) to activate the heater wire to release the seal to physically enter the safe box memory containment section of any PFN/TRAC System. Figure 15 following this drawing is also using 1000 series numbers. This is a certified seal placed on a sensitive area by the appropriate authorities to prove an untouched record keeping for accountability. 1025 is the security relay switch and can be a silicon relay with a gate lead 1033 or a standard mechanical relay where 1033 would be one of the leads to a primary coil the other terminal would be connected to the opposite pole in this circuit. 1026 is a wire or thin piece of conductible metal covered in a substance that will melt when heated to 300 degrees F or something less (application specific) the prototypes will use a product call polysulphone which is a heat resistant plastic. The inside of a PFN should never reach this temperature as it is insulated.1027 is the plastic well anchors.for the seal with galleys to accept the liquid plastic during an authorized installation of clean memory and the removal of a untampered memory component. They are positioned structurally around the access door and are stamped with an registered ID number for legitimate access to this compartment. 1034 is the negative terminal and can be provided a contact terminal or wire to ground in the automotive applications. 1035 is the positive lead and it too can be provided a terminal or wired to a fused positive lead with the appropriate hard wiring and fuse amperage. 1030 is the negative power lead and 1029 is the positive power lead. 1031 is the processor and can send the appropriate signal to the gate circuit out fitted with a 1003 trickster circuit that is resisted to a set signal, or the processor can energize the other side of a mechanical relay 1025 and there by turn on the current and melt the plastic seal. Or 10 32 can be used to send the correct electrical signal to switch the security relay 1025 and it's resisted trickster circuit also energizing the seal system separate of the processor in the event the processor has been compromised.

Figure 15

Is a physical view of the PFN secure area for memory storage. This drawing does not depict any specific guarded area it is used to show the physical locking of the access door and the seal going around through the anchor seal wells 1028 SA. 1036 is the physical lock throws through the side of the PFN. These can be operated physically and or electrically if so desired. 1037 is the key slot cylinder and this cylinder can be constructed like the new

ignition cylinders and outfitted to read a resister chip in the key to activate the SR part 1025 in Figure 15 and melt the seal the seal is 1036 and it goes around the entire access door. And 1038 is the secure box itself.

So there will not be any misunderstanding the PFN box can provide interfacing protection and security to a lot of electrical components and personal property items, however the memory storage and any circuits responsible for TRAC routing will be electrically secured and physically secured in the certified or sanctioned area with lock ans seal to protect the memory at a legal level for evidence and or any legal proceeding

Figure 16

Figure 16 is a list of U.S. Government Agencies. And in fact it is actually a U.S. Federal Government Agency Directory prepared by LSU in a search engine format web page with hypertext and or mosaic or gopher software architecture so that the browser can click on any under lined department or agency and go directly to that specific departments home web page.

So obviously the agencies already exist and they are set up to enter data on to the net through their own web pages. Many of these agencies already prepare data by regions if not states and local jurisdictions or geographical boundaries. Some even provide this data presently to universities, corporations and or governments. for their research and knowledge as well as the general public. Most importantly the areas dealt with in this application as to watch dogging the environment is well saturated with governing agencies. Those dealing with the environmental, law enforcement and transportation as well as all taxing agencies and revenue mechanisms and government spending or disbursement of public funds for the local state and national levels are also available on the Web already. This makes the goal of setting up Web Account pages for local state and national very easy by maintaining a structure that will interface with the government agencies and financial markets supply it's information to this format. The purpose is to develop a public product for rapid awareness of one's physical and economical environment from the local to the national level to greater insure the wise use of technology investment and create a more politically interactive public that can voice its views economically and by public comment through electronic polling in the most efficient and clear way.

Some of the national environmental agencies that would supply data to the web account pages are on page 3 of Figure 2A NESDIS,EIS,NCDC,NODC and the coordinating agency Office of satellite Data processing and distribution. Some more are NMFS,NOS,NWS. As well as the office of Global programs, The office of Oceanic and

Meteorological Laboratory, Air resource lab, Climate Diagnostic Center, Forecast System Lab, geophysical Fluid Dynamics. Many of these would be coordinated By EPA and the data would be presented in clear accurate packets framed to current issues if appropriate, as well as, given as raw data hyper links that the individual can click back on and find the agency and person responsible for posting a specific data framed for a issue.

Along with posting data to the web page many of these agencies would be gathering data from all the PFN's through either their area local phone nodes or networked commercial servers that transferred data to their local nodes. The agencies would then share it and store it and post it on the web account pages. They would be retrieving this data was mentioned earlier from their regional phone nodes and or commercial servers that would be passing this data on to them automatically through special software structured by these agencies. It would therefore be a requirement of any commercial server or any provider that acted as a gateway to any government data management for a agency that they be running the agency approved software to be licensed operator Commercial servers, e.g., cell phone service, etc.

On page 18 of the Directory listed half way down the page the Federal Department Of Transportation has all it's divisions listed and of course these too would be responsible for the gathering of Data in their traditional way as well as through the inventions (PFN) data transmissions, especially in the interactive highway systems.

However, all agencies record their activities geographically but some don't report their issues and/or activities to the local level and the public is forced to track down this information. Ideally with the local state and national public account web pages on the web, these regional agencies can post local data and issues they have collected and are working on as they prepare their data for reports to the regional or state as well as, national level. Of course there may be a need to pass some of this information through a security protocol program first and then post the data in a clear straight forward manner for the public with FAQ's.

Other areas to retrieve data from the PFN and post data to the Web account pages will be The Department of energy, and all their projects and programs starting on page 9 of this register, ultimately all agencies in their mass data management and storage programs would structure there software to support their representation on the web account pages so they can account to the public for their existence and their activities. And of course the Justice Department starting on page 15 along with all the earlier mentioned FBI programs would be an important part of the spider eyes program in reporting criminal incidences that are under investigation so that the general public can also help locally and nationally in the process to jointly police our society any policing process.

These would be posted locally as described for the San Antonio Police Department, etc. as well as supplied direct FBI regional and national Data for all 4 levels of the web account page) And of course this is a main objective in providing these web account pages to the general public. If the individual is going to be ask to share some of their rights of personal privacy for a better, safer and more informed society than it is only fair play to insure they have as much freedom and security as legally possible to all gathered information and for all gathered information.

Figure 17

Figure 17 is the entire inventions control system from the Primary Focal Node and Trusted Remote Activity Controller on every piece of equipment to all accounting processes of public government in every agency desired to an accountable presentation of this Data to the public in general via local state and national Accountability Web pages. It is the PFN.\TRAC\MMN.WWW A social economic and environmental technology accounting system for Democratic Government through a responsible free enterprise system with all the security controls necessary to provide accountable remote and automated services world wide.

At the very top of the page is a group of ten icons symbolizing where the PFN's would be utilized. These few representative icons are by no means to be interpreted as the only places that PFN's will be utilized. They are intended to be used in some form on all pieces of equipment and or placed any where it is determined their needs to be monitoring for public safety after meeting any necessary legal requirements for their installation.

PFN's can have more than one purpose, e.g., they can be used to bill for service or a particular service of a machine and simultaneously be gathering data on an incident or accident even controlled by off board control systems. In fact, as machine messaging continues to encroach into the vehicle and equipment world the more necessary and easy this inventions Primary Focal Node will be to achieve to govern and organize all these systems.

The icons from the top left are trees with a (PFN) box to monitor the environment, weather, air pollution, etc., either sensors or video camera or any number or types of sensing devices. This box is given a squiggly line to indicate a wireless transmission. Once again these monitoring devices are in existence presently, so the invention will add communication to them if they do not have it and return their data in real time to the agencies that are to govern them and any private or commercial operators of this equipment could be given a tax rebate. The agency will then pass the data on to data management for posting, CCing and any proper storage determined by any governing software. The PFN's software will be configured to retrieve the data in an easy to handle format to simplify this process. Part of the accounting

system is to be able to support this mass data acquisition system with out breaking anyone group, e.g., the individual, the governments, and or any commercial enterprises. So to be fair and because every action is electronically traceable in the message headers if anyone's vehicle or equipment is used to capture video for the publics business they are credited for the services and if a news or commercial enterprise wishes to use or tap into their systems to show, e.g., a traffic tie-up then they must pay the owner of the vehicle or not use the data gathered unless the owner complies with a request. The owner would be notified if their system was being asked to use its data link for sensors for any commercial request or the owner could call in and offer location viewing to the news agencies. This is done to accurately pay for the advancement of this extraordinarily large monitoring system.

The next icon up on the left is a generating plant and it shows a direct black line going to the commercial servers semi circle. This is a land line phone link and also a squiggly line to indicate a wireless transmission if needed as a back up or more cost effective modality, etc. The invention could list here all the standards for air quality for SO2 point source standards, particle point source standards, NOx point source standards, all the green house gas CO2, etc. However, there are government agencies and private watchdog groups already involved in monitoring this and they have established standards which can be used a s a starting point. The invention will house all the appropriate sensor arrays to detect these toxin or just the "Nose a NASA development along with a communication link to these agencies to insure real-time compliance and report any amount of violation. Much of this data already exist and can be easily prepared for the web account pages.

The next piece of equipment is a bulldozer and most of the time there is a limited amount of construction equipment but because they are forced to work in dusty environments and therefore are incredibly susceptible to clogged air systems which causes an increase in rich unused fuel being partially burned that deliver a great deal of pollutants into the air. Farm equipment as well, is inherently a dusty environment and also these pieces of equipment are in many cases working with food products and should be monitored for toxic fluid loss as well as any storage tank facilities for fuel pesticides and or concentrated fertilizers. Both construction and agriculture will be serviced in the most part by wireless -pagers with small short range fm transceivers and processors as described earlier. The RF transceiver is for networking all monitored farm equipment to one land line, transceiver where ever possible and the pagers will be used for inexpensive longer transmissions, also this will provide for the repeater function of a short range signal to a long range transmission or telephone communication line, e.g., people locator (Child find). With every land based line so outfitted with a transceiver an emergency network could be developed making every land line part of

the repeater net system coupled to all vehicle PFN's. The short range transmitter would have the same one tuning crystal the same as the tot spot system mentioned earlier this would be a specially dedicated frequency by the F.C.C.

Also other crucial Agricultural Data gathered can be sent immediately to the government agencies to monitor and advise the farming area. some GPS systems are employed by Archer Daniel Midland (ADM) for the governing of irrigation and crop monitoring from satellite systems. Along with the equipment and ground monitoring thee systems could be interfaced to return accurate crop data back to the government and to send aid and services to help a farmer or farming district in trouble due to weather or blight etc. When this was done the farmer could be given a tax break with respect to crop investment and loss. Also if the data gathered in a specific area was used for public use or commercial use the farmer could be reimbursed for the access to their electronic gathered data.

The next icon is a factory and depending on how many pieces of equipment and the proximity they are to land lines these pieces of equipment may also only have a short range radio transceiver that is in communication with a secondary node with in the company (land based line) and reports directly to a company control system in which these machines are monitored and recorded for their operations, but can also be provided instructions from plant management directly to their operators or are operated robotically without operators. This in house network system could provide a data link for service contractors and show a history of operational readings which when run through their software diagnostic programs and or those programs owned by the factory would limit the repair choices and suggest the materials needed to effect an appropriate repair. This would be a great time saver and money saver. Also personal calls could be routed to the operator without them having to leave their machine to answer them.

In the material handling industry many robotic order picking systems already exist and converting them to collect emissions data toxic fluid loss as well as gather performance data would be relatively easy. As well as, store the data either on board each PFN or (existing converted remote control systems) which would be able to store data either on board the machine or in the secondary company node or the commercial service company or any government monitoring agency or any or all of the above.

12 O'clock on the drawing there are icons for a boat and a car. The boat would have sensors on all toxic fluids and in the bilge to determine if the fluid had been passed back into the environment. Having the PFN on board would be a great way to increase safety and to know navigation location at all times. In areas where cell phones and beepers were unable to communicate either a satellite or global digital phones might serve as a replacement. And

also marine band radios would be used. And in this case the radio receiver station for the coast guard would receive a data link transmission along with any voice with the boats ESN or registry and a full report as to it's mechanical condition along with any SOS broadcast automatically sent or initiated by the boat occupants.

The car icon is very well described in this whole application and is used to describe most all the PFN's properties and qualities in all the other industries.

This is also true for the trucking industry the next icon at 1 O'clock. However, just a moment will be taken to point out that the intense concern for air pollution due to the trucking industry Commonly referred to as the colors of smoke blue, black and white. These smokes could be monitored in real time as well as the charging and paying of all fuel taxes and highway tolls. This could be paid electronically without creating toll plazas and the traffic tie-ups that accompany them. merely have a standard signal sent out by the highway computer that requested every vehicle via short range transceiver to broadcast its ID ESNVIN back or to call it in on a cellular highway node system. The ESNVIN would also have a special tariff smart card number already swiped into the cars PFN which was bought earlier. this national card only pays for tolls and gas or use tax or commercial cards can be used when they are accompanied be encrypted transmission and reception for security. And, of course, for the interactive highways or any smart cars to be a reality for society they will need to process all their remote control instructions through a secure PFN that can record and account for all the robotic actions for any legal decision involving a driver accountability and an automated systems liability.

The railway trains and subways, etc. already have many monitoring systems or networks. These systems would be tied into the all inclusive network system to account for energy use and environmental impact. And they might carry these PFN systems in addition to the ones they use now as a back up or all these systems will be universalized but only be specific as to the jobs they per form. At 2.30 on the drawing there is a picture of an airplane with a radio signal from the plane and a land line signal to the tower. Here pertinent data from the plane could be logged into the MMN from the traditional FAA black box set up to down load on landings and during service or this data could be downloaded as is discussed in servicing equipment in the third application for the automobile. The tower and or airport facility is normally well endowed with environmental and weather sensing equipment and all this data would be also segmented by agency protocols and CC for the proper mass storage and also presented in the public account web pages. Also at 8 o'clock on the MMNWWW local node gate way protocol is a icon for the interactive high way and in most cases this will act as a primary local node to down load any PFN data that is standing ready for data transfer

in the PFN Buffer an has been CC to it's PFN's unit storage.

There are in the upper portion of the page, eight concentric semicircles, which are layered protocols established by government standards for the data acquisition into their systems for processing. Their could easily be added more layers and most definitely will, but these eight will suffice to demonstrate how the system will process the data.

The first ring is the commercial communication server and MMN gateway via Land line systems. More and more in the future standard phone systems are going to have faster switching and for any one to operate a commercial node they must have all their phone support lines be Asymmetric Digital Subscriber Lines (ADSL). The second ring in and the first ring provides any emergency service if the PFN did not call or was not able to reach an emergency service phone node for some reason. In this case the commercial server will maintain any and all contact, e.g., voice and data links till the customer is served or connected to the emergency personnel, otherwise the second ring can provide any number of services from making web connections to down loading entertainment packages for the board driver. The next three smaller circles are for energy accounting and environment, transportation and traffic, and the criminal incident reporting system.

It is important to remember in all these systems used in the MMN for the most part they are two way capable in communication and definitely all those used in the spider eyes program are two way. This means in the protocol for reporting crime all reports will be time and geographic stamped and will be reported in real time if certain software is triggered in a PFN or local law enforcement will be able to remotely activate any number of vehicles or PFN's they have recent reports from or any that are in use and giving out a signal to a local cell so that law enforcement can activate cameras and appraise an area in which they have just received an incident reported. Of course all these protocols have to be approved by the public and decide on how the billing will be assigned and credited.

The voting node allows for the public with their special pin Id to vote on the road or in the home. Originally first to respond to issues as they drive home to let their representatives know how they feel on the issues that are at hand. They can view them in their cars on LCD screens or see by hologram wind shields, and hear data delivered by voice. (Not Radio) This system would be developed to sanction a vote with a positive finger print ID and or an accompanying pin code. Also a driver could send a voice mail that coverts to a written message to address an issue on, e.g., area roads and specific conditions.

The two inner circles will be a continual running account of commercial and public cost and gains so an area can judge how well it is doing and also to determine where best to invent or create its finances and use its resources. This data would primarily be gathered over

land lines and this accounting system could be used to make cases commercially to communities to lower taxes or provide support aid in a lean time or help to retrain workers in an eventual lay off. This is not the way business is done to day but it should and could provide a better way of life without stress for all in the future. Business would learn it's local community can help guarantee its survival even if it has to change the way it is doing business.

The inner center of the top semi circle is local government and all the way down through the center of the drawing is government with three pegs interlocking the local government the state government and the national government with the local account web pages that are displayed as local, state, national and international web pages. The pegs have letters in them and they spell out REPS for representative or the elected officials. With the public much more interactive with government at all three levels; all officials in all three levels of government will have to become much more interactive on all the issues and this is why reps is spelled out interlocking the levels of government as another medium by which decisions will be condensed and justified to the public. Basically the objective here is to integrate the process of individual power and responsibility for any one representative to be directly responsible to the empowerment structure held by the public individually.

At 3 O'clock in the center is the state government and below that the national government which are inter locked with the mass data management and storage network. To the left side of the system is data input for the state and the federal government. All the eight semicircles feed data that is presented to all citizens in the same manner unless security protocols have dictated a different path. The two inner circles provide in real-time the financial cost and gains and representatives and citizens can view this information and the representatives can make policy on taxing or crediting back or providing aid and the rest of the public will have the opportunity to completely see this transaction and voice there opinion in real time.

In between each section of government is an accounting process all the way to the federal banking commission. All the data is accounted for so that the financial and economical controls can be better balanced to meet the needs to provide for its society while stimulating growth.

The lower section semi circle is the delivery of data to the web account pages with government numbers on money spent and received locally, in the state, and nationally, Stock reports and financial reports on the local commercial companies, the regional companies and corporations, and the national and world stock markets.

In the bottom semicircle there are four web account pages that anyone can access

from commercial servers communication data links, the world wide web or mass media. Most all of these support response back systems even cable TV with a web box, although there is still a lot of problems getting service to all citizens so access could would and should be provided at any responsive PFN that supports a video display. And in public places as well like police departments and libraries. The four web pages would list issues plainly for the public to view and respond to. And their would be a section to frame issues in which the public could start a question. Also there would be a Yeah and Nay section on issues that were up for a representative vote. Also, there would be data given on the environment, the highway systems, the recent crime and much more vital information. This would be determined by the issues and events that were current first and then anyone, who wished to have data to explore their theories, e.g., on global warming would have at their finger tips all the data and expert opinion as well as an auto tutor to learn understand and relate their informed opinion back to the rest of the world.

The Figures from left to right at the bottom of the page are agriculture being remotely controlled. The highway systems being monitored and ultimately remotely controlled, The car is receiving remote service and the house being monitored and for it's energy use. The computer is a web access, the TV at 6 o'clock is mass media with a web response box. The factory can review all that is on the web as to the public opinion and government policy and the world receives all the data from every where and all the world populous can see how the planet and the other humans are faring around the world. And for this to take place all the national governments agencies must clear the data to be freely posted. Well at least they can start some of this.

Figure 18

NEW FACT CHIP

General purpose possible modality

The Component FACT can be in the form of a physical micro-controller chip or smart chip or it can be imbedded as essential software programs or commands (engineering discretion for components and products). In either case a devices software or firmware initialization command string that is needed to activate any operating programs e.g., (windows level programming above BIOS but only leaving special DOS access commands still functional and or the same or more secure for any improved operating software in the future). This point of operational interception would control the operation of any component, or device in the PFN or attached to it e.g., (activity controls, communication devices and audio systems etc.). The only initial responsive data any accessory FACT component could

transfer would be ESN or identity information to the PFN Trusted Remote Activity Controller processor. The individual FACT component is integrated and or interfaced with any silicon switching relay and or every power regulating circuit or it can send the necessary command data to signal the FACT accessory, component or device to go into sleeper mode or to turn off, or to operate at any level remotely directed level or fashion by the FACT registry and or any preprogrammed protocols. The FACT chips or system programming will be installed as an integral part of programming at the manufacture or the boarder or by custom clearance centers of any given nation state as is determined best and or efficient by the governing authorities (or a combination of both) for any and every electronically controlled piece of equipment, device and or commercially available circuit that can be interfaced in any PFN to be part of the TRAC, FACT system including FTP, CEW, etc. as is made available The FACT system will be able to interface into any control circuit and restrict operation through a chip or embedded software and direct all input signals and out put commands as well as preserve these commands to a designated onboard memory that is also provided time, date, location and the author of command (pin fingerprint ID or iris eye from the FACT registry) as well as the command strings and all responses there to; be they automated or due to human activities. This same data will be stored in a remote redundant storage, and all the same identification and system data for the FACT component will be stored for the new user or installer at the point of initial activation. During normal operations if the resident FACT programming running in the PFN Trusted remote Activity controller is satisfied by a FACT components startup initialization string as normal on board polled inventory components no remote FACT registry contact will take place. All FACT equipped accessories will ultimately have an anti-tamper program that will activate and notify the FACT/TRAC system to notify the registry on power up, if an unauthorized person tampers with out the correct key codes to alter any of the FACT program (ID/ESN, SN, Initialization string and or command functions. The same is true for a self diagnosis program for mal-functioning devices. (Notify either a service center the PFN owner/operator and or the registry if so preprogrammed to do so.)

The individual software will be capable through PFN interface communications to provide their stored data (firmware or flash memory) to the National Registry upon a new installations and will be able to immediately in real-time report this data. Once the data is receive and processed it will be checked to see if it has tripped any alert flags. If there is no criminal or suspect security flags the registry will record the new FACT component installation with accompanying (PFN operating inventory)to the appropriate PFN file in the main registry's mass data storage and apply the appropriate taxes and fees for the product installation and use in the correct geographic area. (registry will be nationally networked, but

can be operated locally if governmental structure mandates this function for tax collection). This will be accomplished through a publicly provided registry phone nodes or a licensed and bonded commercial server that is registered and periodically inspected and reviewed to have and provide a secure Data Base gateway Connection to an intranet (IP) or encrypted Web connection with the appropriate government agencies (the National Registry, FCC, FBI etc.). This is all part of the Trusted Remote Activity Controller System. This FACT program will provide a secure command string and access path from the origination to any mass memory storage system that is search-able from the National Registry by any appropriate authority or agency. Some Fail safe security for the system is provided by the component software of FACT at the application level establishing a handshake with local memory in the PFN and legitimate remote registry equipment with a secondary integrity check from prior legitimate registry contact data. (Possibly a Random code number established in the last contact between any specific PFN and Registry to secure and certify all re contacts as genuine and legitimate un-altered PFN/TRAC links). This would be apart of any initial communication after a com-link was established.

The registry will provide all public providers and commercial servers with the alert flag data so any receiving system will be able to inform the PFN of national security alerts for potentially dangerous devices (terrorist altered components that could be used to activate explosives, chemical, or bacterial or viral microbes contaminants) through the commercial (PFN) remote and management control systems. Of course the appropriate authorities would be alerted to any of the national security high risk installation attempts in real –time. The immediate action could be performed by either predetermined automated protocols or by real-time commands handled directly through the appropriate authorities. Because, the exact piece of equipment can be ID by it's FACT chip along with all it's Original Equipment Manufacture OEM's firmware (Lot No. and any security codes, etc.) and of course this would be updated by any additional or subsequent use such as re-sales, retrofits or re-installments ; an accurate record shall be provided with in the chips firm ware or flash memory, (the PFN/TRAC memories onboard and in the national registry(mass storage to be either provided by public government or commercial servers licensed). This process will be readily supported to provide tracking for commercial trading of legitimate products (new and used) giving government the economic taxing tool for real transactions and real-time product use for new and used devices components products and total equipment packages such as (cars, etc.).

This will also allow for immediate component analysis for any criminal activity and a clear record of component ownership and use through PFN /TRAC/TRACS/FACT programming. TRACS/FACT programming will be issuing Stolen alert bulletins, and or any

security alert flag at periodic times for PFN's to do internal integrity and security tests as this information is reported or becomes available. Otherwise, any device, system and or component will be assessed for it's legitimacy and real-time use at the time date location of installation along with the PFN ESN and what ever other data is determined to be applicable. At this time it will be appraised and billed to the responsible party for it's use and impact on society, it's infrastructure and the environment. Obviously it is necessary to identify the host piece of equipment, and, any and all components the new installation is interacting with, as well as, all interactions from communication devices, control circuits, actuators, and responsible monitors, control and or management centers all of which is recorded in the PFN secure memory (recording devices) for (accountability) and in at least one remote mass storage facility for accountability.

The primary purpose of this singular identity component chip is to track any and all use of the attached device and or component that it has been incorporated into and to report any and all data in a complete and integral fashion, as prescribed by any code, regulation, law, and or standard decreed by any sovereign or governing authorities all as part of real time programming or preprogrammed protocols running in the local PFN/TRAC system or the registries (either local or national, etc.)

Number one position (left) of the octagon is the individual ESN or the Electronic Serial Number ____ each accessory or interface FACT component will have it's own ESN or Identity program and will be entered in the Fact registry at the point of manufacture and will give its ESN program to the Local PFN on every start up and given to the Registry at any new install or recognized alert status protocol flagged either by the component the PFN or the remote registry or service center.

Number 2 in Fig 18 can be like the SMART CHIPS and or a magnetic strip and would provide as part of the components unit packaging and or as a bar code so that an immediate physical check of the component can be search either by a OCR scanner or a hand held magnetic strip reader, or IrDA, etc. With the more extensive amount of data handled by smart cards and chips this is another inexpensive modality that will help in tracking and reporting stolen materials. A hard or plastic card would be issued to the purchaser of any TRACS/FACT device so that they could scan their stolen property data to the National Registry immediately after a crime if not through their existing PFN any gateway node to the FACT registry's intranet. (personal PFNS store Credit card scanners, credit card Phones, or voice recognition systems)

Number 3 is the universal plug and play buss inside the PFN containment that creates the electrical interface platform for all the components. This buss will carry the appropriate

power connection and control connections from the PFN/TRAC/FACT controller to activate, deactivate or specifically control any and all components. Power can be cut off to a specific component through the BUSS or it can instruct the individual component's FACT CHIP or program to intercept power (power input or regulator circuit.

All the electrical connections in vehicles and equipment are need of standardization and I have written to this in all my previous applications and these are areas that will be a standardization effort in each industry and or application specific use of accountable remote and automated control. I have addressed how to complete these functions with present hardware connections firmware and software and have created some new modalities to interface all the present devices. However as shown in Figure 6a the components and technologies are merging and this universal plug and play BUSS in the PFN is an ideal way to make compatible this electrical interface platform.

#4 of 18 is just pointing out that the individual component FACT CHIPS must provide firm ware or stored data of identity, OEM data, last application, etc., to comply with any standard or regulation developed for a national registry or any such security system. Because FACT is a major part of the main operating system in TRAC it's software is also modular and can be in any form or hardware application. The hardware chips and firmware modality detailed in this application should in no way be considered the only modality to create a nation wide security and management that is capable of real-time control of individual components, devices, and equipment. However, any other modality should be considered within the nature and scope of this invention. And this is area #6 of Figure 18. The chip also can perform activation and deactivation of the component and that is what is meant by saying it "must provide control"

Note: While in the description of the FACT component in this invention is described as a chip, this does not have to be the case. And the best form of data management for security is open to each individual manufacturer's best options with their particular products to provide this function so long as it is approved by any governing standards for this use. It is obvious that a physical chip could be replaced or compromised in it's firmware so additional means will be utilized to insure security

Such as the random code exchange discussed above at the last legitimate contact or string of contacts with the Registry allowing only appropriate one way communication at the time for the PFN compare list or component compare list is running to validate a legitimate registry contact or vice versa for the registry computers being accessed by a new PFN component application.

Figure 18A

This is a general flow chart of a self contained PFN/TRAC/ FACT management system that will be utilized by every piece of equipment. PFN's may have all the listed components or any number of them,; however no mater what is electrically interfaced it will have to be approved and registered as it is activated or deactivated. The very first triangle at the top numbered 4-500 refers to the one and two way pager systems detailed in the Figures 4 and 5 of this patent application. These pagers as is true with all components will ultimately be provided FACT software to identify their activity and especially for those technologies that are responsible for providing communication data for remote control.

The second triangle is for cellular phone systems and is completely detailed in Figure 6 as a more sophisticated communication system capable of handling and delivering very good data signal in volume and quality for applications needing such quality such as real-time video, etc.. The 3rd triangle 0- infinity frequency refers to any and all kinds of Radio Frequency equipment (including cordless phones and high quality and high powered RF equipment equally capable of providing large data streams modulated on their signals.

The 4th triangle with the word locate can be either cellular phone poxcimetry tracking, GPS, Lorands, LoJack or par of any interactive highway controller system or master surface transportation control net work and system receiver and or transceiver. Along with this locate system triangle the 5th triangle is a miscellaneous communication receiver and or transceiver that is responsive to light, sound or any discernable electromagnetic wave or transmission.

All of these PFN communication triangles devices or modalities shown as upside down triangles are not shown in Figure 18 as having a FACT chip but they would also be provided with FACT software to report their activation and any specific role played in any remote controlled event as either as a receiver and or any type of transmitting device.

As is evident in the drawing they are connected to #1701 which is the uni-buss connector to the PFN/TRAC control system and accompanying memory storage units. 1702 is the Trac software with it's resident FACT software program. This fact program can be updated and it is capable of storing and retrieving data back from it's accompanying data storage. As detailed through out earlier related applications these PFN control circuits are sophisticated mini computers with extremely efficient processors in the for of euro 100 boards. . And as explained in Figure 6 all these technologies are merging an the improved capability and speed of processors is in the major reason for such enhancement. For this reason I am claiming that these improvement fall within the nature and scope of this invention to provide accountable remote and automated control for society and it's institutions. TRAC

is of course the Trusted Remote Activity Controller a modular based software program of which FACT the Federal Access and control Technology is an intricate part. These programs are run by the PFN min-computers and they send their commands and direct the data received by the uni buss to the appropriate data storage. Either a hard drive or the specially preserved non-volatile FACT memory that can either be down loaded or physically removed to be used in a court of law in the proper manner as determined by any rule regulations or laws governing evidence and it's acquisition, preparation and presentation for a society.

Both on the left side and right side of 1801 uni-buss is all the interfaced controls Accessories personal items and electronic possessions and alternative data communication devices. These devices are coded in the upper corners with the initials or first letter of the words that describe their boxes as examples of connectable interfaces employing the individual FACT Chip. This becomes more evident in Figure 18 where the bottom of the page supplies numerous octagon stop sign shapes filled with these same initials indicating FACT applications and tracking. Also before leaving Figure 17 it is important to remember that in the ram memory of the mini computer the Fact ESN will be stored for all memory devices and the memory will always require the processors ESN or any comparable ID technology for any further or final review by the appropriate authorities or to comply with any legal proceeding.

It should be also understood that this universal Buss can extend outside any protected area with the immediate electronic protected capability to recognize and protect against any deliberate shorting or questionable interface. At the bottom of Figure 18A the universal buss illustrates it's capability to handle power as well as in put and output control transmissions. It is also important to make clear that this involves a universal secluded antenna buss or reception will be provided for by certain types of physical structural elements in the PFN's structure to allow for patch antennas or physically small profile antenna structure to function with in any standard regulation or legally prescribed manner.

Figure 18B

At the top of Figure 17 there is a box to the left called the National Government Activation and Check System. Form there - there is an arrow showing a Data Base Connection (DBC) or a world wide web Internet connection (encrypted if applicable) with the number 300 above indicative of any local and regional network as is evident between the left national box and the box on the right side of Figure 18 which is termed Local Government Activation and check System. These most generally are the primary sources to supply data and or to act on any data receive that involves National Security, Public safety other than

individual input which in most cases is provided to either one of these node as would be any international requires, which will always first be edited through the appropriate national authorized channels. The National Registry will be a large routing system for mass management with only a system processing storage protocol and system that will handle data in a prescribed and secured manner through any and all of the 6 transparent IP layers to the appropriate seventh application layer detailed earlier where it is transposed by the application encryption to insure security. This will be the same for all forms of communications wired and wireless as they are processed through their respective communication nodes and gateways (licensed Providers and Servers) to land lines, fiber optic cable systems or land cable systems.

The center three blocks are the facets and functions of the national and local registry for government, to develop security for all in the nation and to provide better public safety and to build trust within all of humanity, because of accountability and fairness. This is a safe guard system for man and machine messaging that is accessible by all of a nations society first individually through internet connections and if not accessible at least by any portion of humanity accountable to all involved parties through comment or constitutional procedures provided in the TRAC/FACT software. Internet dialog and media awareness for all types of media (mass and individual) as well as responsive and public access and input will spawn a much more involved individual citizen and functional democracy.

The first center block is termed AUTORIZED INSTALLATION REGISTRY. This may be a network of secured computers in different locations or it might be one system in none location. The inventions purpose is to create realistic functional modality that can create this national and local registry level of accountability presently out of existing computer systems and to project some future consolidations of local nodes for related activities and data to help structure efficient data communications for all the government agencies an commercial services. The Actual structure of course will be part of a large standards effort and civil legislative effort.

Total purpose goal:

This is the base system to create a national directory of all products sold and re-sold in a country to better track their impact on economy, resources, environment, health and infrastructure all around the world and at the same time to allow nations to have a FAIR frame work to develop and use imported products, which are needed. The PFN system can help to develop trust to insure an accountable answer to all of Societies legitimate concerns first for individual survival and then to be part of a mutually healthy co-existence with all of humanity, and all forms of worldly life.

The Authorization Installation Registry function is to record and make available by request and or to recognize any PFN use of an electrical device in conjunction with the PFN and first run a compare function to any and all legally known produced, and legitimately marketed products in a legitimate sovereign locality through local and or toll free telephony or RF or MISC. communications technology employing isolated network connection and or the Internet (IP).

The authorization installation will require a complete OEM specification and description that can be used to specifically identify individual devices and or components (Requirements to be determined by the sovereign authorities). This data will provide depreciating value levels and integrity checks that will be beneficial in tracking use and varying performance for securing public safety. Also the depreciation schedule will enjoy a diminished cost of operational tax relevant to the products prior use and or time of use. This provides a use tax not a sales tax for governing structures to apply to real time use. This frees the Internet to trade and free communication for general transactions and allows for the legitimate taxing structure for actual impact on society's infrastructure and environment by machines and the work they do

The second block is the Restricted Authorization or Crime Registry. Once again this data is supplied by everyone and anyone but primarily cleared and reviewed by the national and state or regional governing agencies. The really great part of this section of the system is that the private individual can in real-time participate in a personal injury theft by telephony with scan data or through personal contact with law enforcement agencies. With total accountability all parties will have to face their own actions in the proper legal settings. And basically there will be no use or miss - use of stolen property.

Of course this can be done for resources and all things needing monitoring to insure any fair deal is lived up to and or is humanly reasonable.

The third center block deals with the communication capability. Ideally this will be accomplished by toll free telephony or RF nodes for the public in using the publics privately owned equipment and PFN link ups as a hospitable commercial service with all other gained accessible service options and provided free by government or public providers for the tax and public interest previsions.

The 4th block in the center of Figure 18 is the centerpiece of my inventive technology for each individual piece of equipment in this machine messaging net work.

It is the Protected Primary Focal Node or PFN created as a protected electrical interface platform to merge, focus all host equipment's accessories and component's power and control circuits into one local accountable control and communication center. This PFN

on every vehicle or piece of equipment is then linked, coordinated and managed with all other machine use and activities by a greater mass communication and management set of computer network systems (through RF, telephony and nodes or gateways) either for surface (land and sea) coordination and or for aviation.

However in this Figure we are concerned with developing an understanding of the FACT software in the PFN and or possibly individual CHIPs that are at the bottom of the page as octagons or (mini-stop signs).Once again these might well be in the form of physical hard ware and read only firm ware or they might be integrated software programs interlaced and inter-reliant on the PFN/TRAC/FACT security encryption both in the PFN and in the National Registry system. Through out this entire drawing Figure 18 there is two way communication form the individual chips or FACT programs to the national government activation and check process. However, the PFN gives the commands to the individual chips via the universal plug and play buss. And retrieves their essential operational data, e.g.,ESN, and or MIN and production Identification and seventh layer application security instructions from the ISO OSI networking Model. If for example a stolen audio or sound unit is connected to the uni-buss of a vehicle. The PFN computer will signal or request information from the individual FACT chip in the sound system (SS-ESN-F). This can either be sent by isolated control hardware (wires, etc.) or by sending a modulated digital signal on one of the power legs or it can be accomplished by short range transmissions if this modality is employed in future wireless vehicle and equipment control systems to ease plug and play capability and reduce the need for so much hard wiring. No mater the means the PFN will inquire for an individual fact chip as soon as it senses current draw. If there is a change in current from a normal operational level the PFN will request and or review vehicle conformations for any trouble codes logged in the charging system or any battery draws or charging problems. This is performed by a TRAC software algorithm

And standard current sensing micro chips in the uni-buss and in the host equipment's electrical system, which can generate either analog or digital signal that the PFN/ processor can receive and recognize through any of the above in vehicle communication modalities. This current sensing system is part of an anti-tamper system of the PFN. It will give driver alerts to the abnormal draw unless an individual component FACT chip sends an ESN and data signal that is recognized for a specific authorization or security protocol. At the very least all components can be individually judged for their current draw and reported to the display or checked against their OEM manufactured specifications (Data delivered by the individual FACT CHIP to increase security that a component has not been altered after manufacturing. Even a individual resister chip like that used in the present vehicle keys could

be installed secluded in the board with the FACT Chip to add even greater security and integrity checks. While this idea is creative and new the technology to make these combined innovation are available as electrical components and any one who is skilled in the art could from reading this section create the necessary circuitry to complete these security tasks. All the components are listed through out my related patent applications for the trickster circuits and the security seal activation switch. The universal plug and play Buss as always stated will have to be a standardized effort for the most optimum development. The little octagon stop sign FACT chips at the Bottom f the page have letters on the top of the sign like AC-F which means (Activity controls- function). These correspond to Figure 17 left and right blocks.

Once again all the components operating in or though the PFN will have to have FACT chip identity capability, communication processors, data storage as well as all these listed that access the uni-buss,

Figure 19

This Figure will detail the registry system in general. At the very top of the page is a small box that says World Organizations. This is the present state of World affairs that the national government agencies should be in control of the data involving any and all mechanized civil and industrial uses of equipment and the impact data. Ultimately the PFN/TRACS system can help to develop trust and fair play in the use of the worlds resources and equipment as well as free humanity in an efficient manner. When humanity matures past survival paranoia to address only the real fears of peaceful co-existing the PFN management system will serve it's greatest function. However now it is best used and developed in the individual nations. As communication and understanding is increased the natural sharing of data will take place and is already transpiring on the Internet. For the present all government agencies will serve to clear all PFN data that is earmarked for their attention through the National Registry and be responsible for it's dissemination world wide. This is why the big black triangle ends up with National Government Agencies. Of course any data request generated by state and local agencies or pertaining to same agencies will be notified and enjoy all the same rights constitutionally guaranteed to day in their governance, but over this new technology.

This is the means by which taxation can be performed directly from every PFN (Sale and or use tax) for the state and National government as has been depicted and addressed in Figure 14 of this application. Also credits can be applied back to the user or citizen for any community service performed by their equipment. Also aid can be applied

with re-education programs carried out through PFN terminals for defunct industries and old jobs that have resulted in layoffs. This has been detailed in Figure 14.

The bottom of the triangle has LOCAL GOVERNMENT in big bold letters. This is done for two reasons. First local node and gateways will keep cost down for Registry network and second regional state and local government is the agencies that impact the individual in most cases. As has been detailed earlier in Figure 13 all the government agencies are now maintaining web pages and data phone nodes and through basic routing using ISDN of Cerent Industry new fiber optics and Cisco systems routing capability these agencies can be given an efficient data management for local regional and national Data base connection and inter agency connections as well to allow for the fast local discrimination of data as well as provide much of this general data on the web for the public on or through the media

Below the local government registry are the FACT Management & Memory for commercial servers. And to the right side the same FACT Management but provided by public provider nodes. The difference being that individual commercial servers will be providing more fee for services from emergency service to computer down loads and the public nodes basically will be for government services. Basically the PFN will use both systems commercial and public. It will do it automatically if it is pre programmed by the owner or it will do it as a directed command either given locally or remotely. An important note is that both these TRACs systems will provide accountable memory as does the PFN at the very bottom of the page which is responsible for activities performed and authenticating the activities. As shown and discussed in Figure 19 land line wireless and satellite communications can all be used in the system

Figure 20

This is a flow chart to detail FACT software in the PFN on a host piece of equipment and also the interaction in TRACs/FACT software programming in the main registry. For a new install the process is started by plugging the component in ideally to the Uni-buss. As illustrated by the second block down the PFN/TRAC/FACT software recognizes the Components Fact chip and calls a predetermined number. The call in number can be a commercial server or a public provided node that access the national registry detailed earlier. As shown on the right half of the page is the TRACS FACT software in the main registry system. This is the national and state government registry system. The call in received by the PFN data from the new component check compares the ESN and manufacture data to OEM supplied registry lists and known crimes of stolen property registered in the registry. If all is

clear the registry approval is given and the transmitted back to an approved registration program in the PFN. At this point in the plug program and play the initialization program in the PFN/TRAC System adds the new ESN to the start up sequence in the PFN computer and installs any software drivers or interface communication links for the new device to function in the present PFN/TRAC system. This software (by manufacture and product engineering discretion) may be imbedded in the devices software (or firmware) or the device maybe accompanied with software to be downloaded e.g.by floppy of Disc etc. or a second number from the registry call might be made to an automated IP manufacturer node or web site for the manufacture to down load the appropriate drivers, etc. and be able to keep track of the devices new service and owner.

In the registry the component is listed as it's appraised value for new or resale value tax taxed and shown on the display for the operator and or owner of the host piece of equipment to approve or refute if provided for and determined by law. The same redundant data is sent to the appropriate governing agency and a tax bill is prepared, unless the operator decides to pay in real-time with either with a credit card or bank debit card via a card reader in or on or attached to the PFN. In any event the entire transaction is timed dated and the run status is added to the inventory list of the vehicle or piece of equipment. If hard copies of the transaction are required a return E-mail address can be sent to a home unit for printing or memory storage or printed on location from the PFN or down loaded to a Lap top and printer or an accessory printer attached to the unibus or one that is resident as part of an application specific PFN/TRAC protocol..

If a component is flagged with an alert it will be accompanied with specific software commands or additional alerts depending on the severity of the situation. A simple theft protocol might activate the unit normally with out notifying the local user and alert the appropriate local authorities to the location of the stolen property to first regain custody of the stolen property and inquire as to how the person gained possession or received the property or as to how it was attached to the present PFN/TRAC system.

If there is a Terrorist alert to a particular component as soon as the person install the unit the alarms will be activated in all emergency responding agencies and even kill all power to the PFN and or set off alarms and warnings. This depends on the nature of the emergency and will allow for on the spot real-time commands to augment any response. As mentioned earlier FACT can provide a stealth eves dropping mode so that operator owner and occupants can not tell that they are being monitored and or recorded but this access mode will require a signed judges order and his personal access codes that are changed by time mode to send this command. Once again any miss use or abuse will of this mode will meet with serious

criminal and civil penalties for the individuals involved and or any agency private or commercial entity. Freedom of information act will apply to any legal owner of their PFN controlled equipment and they will be able to down load their individual memory that will show a complete access and use of their system coded with the agencies ID (local and national as well as for commercial access

The only acception is the court ordered stealth surveilence : or National emergency. All other contacts must first announce their access, be recognized and agree to the process or it must be a time of national emergency, marshal law or a crime in progress for public safety use. In any event all will be recorded and accountability will be part of any process to use or not use the PFN/TRAC/FACT record as evidence in a court of law.

All rights of the individual like, e.g.,the 5(th) amendment, recordings and privacy must stay in place and be applied to any real-time preprogrammed protocols and or use of data gathered in legal proceedings. The exact use of recordings and the preceding announcements or Maranda rights will be part of a legal standards effort.

Also a redundant record will be kept in a remote location either in a licensed commercial FACT server or in government mass storage. These systems are detailed in earlier related patents. As the spider eyes and green eye software programs. The Fact program will basically be operated with the Justice Department the FBI IBSR incident base Reporting system and The UCR the Uniform Crime Reporting system and it will be part of this technologies Spider Eyes system and will be totally accessible to local law enforcement and even the general public through national state and local agency editing as justified.. However all crime activity will be given ID's either IBSR-UCR or local and all data can be retrieved from the mass data in any discovery to make everyone accountable for all decisions and use of data including editing from the public.- MS is the mass storage in the TRACS/FACT system. Basically this drawing is self explanatory and I have outlined in writing what would be incorporated in any software algorithm as well as how humanity will be able to legally use this technology in a constitutional way.

This detailed use of the invention is not meant to determine the exact parameters for programming, but it is meant to initiate the proper questions to be handled by all to maintain a free and healthier society through accountable remote and automated control and management of societies equipment. There are also personally worn PFNS/ TRAC systems that are used directly on individuals (with varying levels of freedom, e.g.,nursing and halfway house or parolee programs)where these devices detailed and also have legal discussions that even impact more on society. The inventor here has tried through out all the related PFN applications to address as an intricate part of the invention the constitutional use of

accountable remote and or robotic control and management for the evolution for humanities technologies and society, while preserving the individual's freedoms and improving the quality of life in harmony with the earth's environment

Figure 21

Although their will be many different software programs in TRAC and in the TRAC's system. FACT is being used here first to handle National Security and High Security Situations and to create more aggressive remote and automated controls with useful management systems, while helping to insure National Security, Public Safety and maintain respect for the individual citizen all though TRAC accountability. The software flow charts in this Figure are being used to illustrate the detail and capability of the PFN/TRAC system. Not all software applications will be detailed in flow charts here or in the related patents, however, from this detailed FACT software flow chart anyone skilled in the art of computer programming will be able to read all the written discussion for this TRAC/FACT software program and easily construct a software flow chart to write a program and or algorithm(to function in the application specific hardware) and perform or complete any functions described in any of the PFN writingswith the hardware detailed. To write all the possible flow charts for this accountable remote and a automated management system would be impractical and unnecessary at this time. After doing several software programs much of the systems either for intranets or Internet would be the same and would be a redundant exercise with different commands only. The other reason for not writing the software flow charts is that the public and the agencies need to dialog on program protocols, regulation and standards for the application specific PFN/TRAC/FACT/CEW/FTP programs. However all the technology has been detailed to create the PFNS in part and or parcel through out all the related PFN applications So for this reason any software, programs and algorithms developed to perform even the written described functions in all the related patents are considered to fall within the nature and scope of this invention and or technology known as TRAC, FACT, CEW, FTP. etc. This invention is an organizational local electrical interface platform tool to provide a set of remote monitoring, management net works with accountable data and real-time control capability for society and it's institutions to use respectfully with their machines, vehicles, equipment, resources and each other.

Figure 21 is a possible software flow chart for authorized Interrogations of a PFN/TRAC systems. In this application it is important to remember as it is true in life situations today that public safety rights of society must supersede the rights of the individual if so determined by the appropriate authorities issue by issue. The one important thing to

remember in any such situation is that in most cases accountability for these activities are not equally shared. It is possible in these situations that they may result in the miscarriage of justice or misuse of power. This will always be a possibility but with the PFN accountability provided by the redundant memory storage functions makes it possible for events to be monitored with a greater accuracy and force to maintain and protect the individuals rights to privacy and integrity and allow improprieties to be redressed and rectified through compensation to those who may have be damaged. Also those responsible can be punished. This process is designed to the PFN/TRAC system to instill respect for the individual as a primary function and is absent in most data acquisition technologies in use today.

Figure 21 is divided into two sides. The left side is what is going on in the PFN and the right side is what is happening in the registry network. Both are running known activities to the driver/operator or owner and both can be running unknown polling or surveillance functions. These are all in a direct relationship to how the law functions in the United States today. The only difference is they happen in real –time at the speed of light or electricity. Therefore they can be more intrusive in an instant and or more dangerous or equally perform lifesaving functions. Accountability and secured professionalism with mature respectful use can not be over emphasized here or fail to shepherd these activities both from the individual's perspective and the authorities perspective. (Abuse just has to be intolerable by all parties and accompanied with the appropriate punishments.)

All government agencies will be able to contact all individual PFNS as simple as calling a number or by punching up the ESN or ID and an automatic dialing process or digitpeating communication will contact the specific PFN/TRAC address. They will be all capable of accessing certain levels and activities of a PFN and any interfaced equipment. These communications are known contacts and the owner/operator of the PFN being polled has the right to deny access e.g., (This process takes place by PFN user/owner notification (light panel or display) and a simple yes or no response with PIN.)(polling will define what type of access, areas, files or activity controls which have to be agreed upon by owner/operator), e.g., a state may poll a car for an EPA reading or other equipment telemetry check. The individual may deny the request and be given a report date to a state facility or if out a state may require a state from the home state EPA check station. This is a benign example of everyday regular business applications. And any number of commercial interests can contact any PFN or people can program this feature out or use it only for family or discriminated contacts.

However, the second level of PFN system interrogation is not under the control of the owner and operator and is a function of law enforcement. It can be performed with or without

consent and it can be performed with or without knowledge of it's function. But it can not be performed with out the proper authorization from the proper authorities and or without accountability both locally and remote. Law enforcement alone is not capable of performing this function-it requires the justice department and judicial branches of government (both local or national as applicable). Judges can view the process and stop it in real-time if their order is violated. The only exclusion to this procedure is a National security alert which relies on the appropriate governing authority and agencies to respond correctly and in as rapid a manner as possible. However local as well as remote system recordings should be maintained for review but latitude should be expected for these emergency actions by all individuals while reviewing their constitutional right to ask for a civil suit and damages should be weighed with the gravity of any particular situation in mind.

This more extensive discussion on the Federal Access and Control Technology FACT which is being used as a model for programmers and engineers to see how the PFN hardware devices and many existing computer systems is being utilized to create a Machine messaging system or network, through wireless RF, telephony and wired IP connectable interfaces for the PFN/TRAC/ FACT program and it's many sub programs like Green Eyes, Spider Eyes, DOT interactive highway. CEW, FTP and all the Intranets or the interfaced Internet can be constructed.

To take a second to describe some of the sensors that can be activated by either the number one or number two protocol are like the HC or human contact sensors used to monitor a persons heart rate BP or consciousness or breath constitutes like the noise or other atmospheric chemical sensors like breathalyzers as a condition of driving for a heart patient, diabetic epileptic known alcoholic, drug user etc. These would be determined by medical and legal staff with the intent to maintain public safety and provide as much freedom and normal social activities as possible. All the programs to shepherd these activities is well detailed in the related PFN applications from local law enforcement to behavioral and medical EMT personnel. But this basic set of flow charts set up the architecture for the PFN device and system for any level of involvement.

Figure 22

In Figure 22, this software flow chart starts in the TRACS System or in the main registry. Here alert flags are generated with the correct FACT ESN and case number for fast cross-referencing in the IBSR or the UCR operated nationally by the Justice Department's FBI. However, not just law enforcement and other government agencies will be able to innate an automated crime report or alert, but also the general public will be able to file an

automated report through area government operated web pages and Internet nodes or PFN/TRAC/FACT access as well as in the traditional manner with the area police department. FACT cards held by the legitimate owner will allow for rapid scan in or card swipe by a magnetic reader. These encoded cards can be prepared and programmed at the time of a legitimate purchase and any and all identifying data will be available to complete a crime report with the exception of listing the geographic location unless the theft was automatically reported by a PFN/TRAC/FACT system as it was being tampered with along with a present component inventory of FACT-ESN or identity numbers sent in real-time at the theft or tamper event time.

The second long box below for restricted authorization and crime registry will process the crime alert report. As stated earlier if it is a theft it might require one type of automated and remote control responses, and if it is an emergency (public safety or National Security scenario it might require another type of aggressive remote and automated control options. Of course the agencies and personnel responding will be part of a protocol set up by the appropriate authorities and governed by laws, rules, codes, and regulations. And of course if the first box above is processing the normal commercial registry of products and product information the normal install sequence would access this data and activate the unit and prepare any tax information and pass it on to the appropriate accounting agencies.

In viewing Figure 22, it is important to remember that this diagram is portraying a FACT scenario for a stolen device or a device determined to be of danger, e.g., like a part of a subversive weapon system to perform a terrorist act, etc.. The everyday use would provide local operator notification from any manufacturer that registered a defect or recall of merchandise order or even perform real-time repair via electronic augmentation or reconfiguration if permitted, possible or required.

Any local PFN/TRAC/FACT configuration will have routing for and to local law enforcement for real-time responses through IP connections, RF repeating or Digitpeating, wireless, telephony and paging systems to handle the detailed Spider Eyes program in related PFN patent applications. This responsive networking as described earlier will utilize all vehicle and equipment audio video systems and pertinent telemetry and tracking data in a prescribed geographic area (boxed and clicked on a calibrated map) to follow a real-time crime, e.g., for real-time recovery of a kidnap victim or pursuit of any crime in process. When a box is drawn on the calibrated map of the control center for local law enforcement a FACT communication signal will be sent out on RF, wireless phone and paging systems so that every PFN no matter what communication array will be instructed to respond if it 's TRAC program determines it is in the geographic area. The PFN will also respond with it's

assets like if it is operating video systems etc. PFN/TRAC/FACT systems will be contacted through radiuses of physical address and by ESN numbers or communication numbers or designations or vehicle tag numbers all through a gigantic compare list algorithm running in the mass data and management systems of FACT and all the related agencies.. Priority in this case is assigned and implemented as a public safety emergency. Other software Protocols algorithms in the PFN?TRAC system will be assigned for general purposes and complete similar routing functions but as service and not at as high of a priority. A special set of protocols for interagency networking and data access or files will be constructed for public safety and national emergencies. Even the investigation of petty theft will be protocoled at a lower level of routing and resource use.

Of course the public and governing agencies have to agree upon a protocol that utilizes essential data and keeps unessential data transparent or encrypted and removes it from the system to respect privacy, as soon as it is determined as unnecessary to the event it was gathered for. The acception here is that some other equally important public safety incident or national emergency issue is disclosed or requires the appropriate attention. "Spider Eyes technology is well detailed through out the PFN patent applications for the original Stop and Control Box commercial offering of the PFN systems including the video systems responsive to the PFN/TRAC software computers and transmission to remote locations. And even the handling of the mass data acquired due to automated application specific surveillance that is preprogrammed in some PFNS, e.g., for an impending collision etc.. However through out all the PFN applications the writing of specific software commands and protocols are dependent on society structuring the legal use,

DOT, Highway Safety NTSB would support a set of nodes in a transportation web for the nationwide web to provide traffic management as part of any interactive highway system directly along interstate corridors. There will be TRAC/FACT gateways and IP connections from any interactive highway system interfaced into the FACT system to be part of an integral part of law enforcement including the EPA. The cellular and wireless telephony system has well saturated their development along these traffic arteries and are ideal components to help provide additional ground signals to assist in automated triangulation in conjunction with or with out GPS data for accurate land platform guidance algorithms running in TRAC. For this purpose these TRAC programs will also process local video data and highway RF beacon data or use the electrical signal form any sensors of magnetic markers and distance sensor signals on board the vehicle to be responsive PFN/TRAC management computer as has been detailed in earlier related PFN applications. Similar application specific systems will be set up for travel on waterways and the high seas and

aviation communication will be tied in as well. This will allow the FAA, DOT, NTSB, EPA, NOAA and the FCC to develop the proper protocols access and routing of communications and up-links in the TRAC/FACT mobile transportation system of spider eyes and green eyes to control, manage or monitor any and all mobile assets on the earth's surface in real-time to limit the amount of collateral damage and any injuries, as well as, alert the optimum response public safety response effort in type and quantity, e.g., fire medical police, military.. Other agencies will be interfaced in to any responsive application specific system like the present transportation system and including this transportation system as it applies to national security, e.g., DOD, FBI CIA and these protocol will be determined in a collaborative protocol effort between agencies. They will all provide the PFN/TRAC accountability and will be accessible on a right to know and need to know basis as determined by the public and the policies they choose to govern themselves with as administered by the appropriate authorities the public has in trusted with these vital responsibilities. The levels of authorized control will be available through FACT on the basis of the need to control and require personal Authorization, Identification and Authentication to achieve command control and all other agencies and PFN/TRAC Screens will display the command control Agencies symbol on the PFN/TRAC displays. As stated earlier protocols as to how these preprogrammed options will be written as software commands is the essential work of the involved government agencies.

A statement from the inventor: Being raised at a time when Audus Huxley and George Orwell wrote Brave New World and 1984 respectively the fear of government becoming to big and becoming big brother has already happened in our present technology. In most cases it is not an organized policy or effort to diminish state rights and even more importantly individual rights, but not for rogue elements trying. So this is a real concern as our technology becomes more capable of individual data invasion and personal remote and automated management or control functions. So the most important point is for people to be responsible and respectful of how there fellow human is feeling about the services and activities of the PFN/TRAC system.

These technology's are coming to the world The PFN/TRAC system has been designed to organize their use and make all accountable for their actions and activities to guarantee there is review and correction But only the emotionally mature development of each human being will insure the proper use to the accident only level of impropriety. However, the PFN/TRAC system was created to be a real-time instrument of the United State Constitution and like the forefathers envisioned and enacted their technique, e.g., the Constitution and Bill Of Rights to create a fair social structure for the learning curve of

human behavior so should our technique (Technologies) be applied to our present time. There is no doubt our forefathers understood the human animal well in how are society has been structured with interlocking powers of checks and balances. So to ensure the most optimum chance for all to enjoy their 80 to-100 year learning experience here on the earth we have to be mindful on our freedoms and our responsibilities to be an individual and to be a society with the use of our technology and in this case how we write the software protocols and programs and how we empower ourselves and governing structures. PFN/TRAC/ FACT is just a tool like our constitution, and the economy. These are just social tools to improve our survival.

NOTE : A separation is being made here deliberately so that legal distinctions will naturally delineate between humanity and machine in addressing rules regulation and laws. Much of the same technology will be used in the same way for both personal PFNS and Equipment PFNS, but when either pertains to human rights vs. machine use and management the data acquisition and subsequent recordings will require special considerations and attention to maintain democracy to insure the UNITED STATE'S CONSTITUTIONAL PRICIPLES –for -WE THE PEOPLE-which –IS OUR BLESSED HERITAGE— and must be carried on in the tradition OUR FORE FATHERS conceived to protect individual freedoms and personal privacy rights as the TECHNIQUE to be employed for this PFN/TRAC TECHNOLOGY—

The PFN/TRAC technique must always strive to apply the principles of respect from society to the individual and from the individual to all of society with accountability the tool of review and handled in the appropriate settings to be constitutionally correct. To develop this technique for the PFN/TRAC technology an on going deliberative process involving all of the public voices; civil, commercial private groups, organizations and government will need to be in place, e.g., local town like meetings and the deliberative process used by the Kettering Institute for framing and re-framing issues and arriving at true public policy wishes may prove beneficial, as well as the use of the standard representative governing process. The Constitution and the Bill Of Rights in the United /States should always be the yard stick by which we measure and construct the technique and application of PFN/TRAC /FACT in our life our society and for all our technology. While, it is greatly assumed that this is the manner in which we conduct business with our technology today, upon deeper review it is obvious that individual rights have been greatly deteriorated as a result of our present technical brutality and ability to acquire data and decimate it, or commercialize it with out the proper respect or accountability or controls. So obviously better manage is needed to restrict the personal damage that has been caused in many cases. In studying history we always say

remember humanities worst or mistakes so as not to repeat that lesson. We all know the what happens to societies permitted to deteriorate the individual and do not respect the individual's freedom and right's to privacy. So accountability in real-time memory storage can be used to remember and create respect through liability and civil punishments. This will also help to can paranoia and unsocial behavior in those that feel disenfranchised. by their government, e.g., recent Wakeo, Ruby Ridge –the Oklahoma bombing, with the build up of private militias. The course of action can be a day in court with virgin evidence gathered locally by each individual's system.

In the case of the United States; it's future lies in it's deep past heritage of all races, religions, ethnic groups and multi- nation state ancestry coupled with the resource of human capability and creativity based deeply in personal FREEDOM. The respect for personal privacy is a major component in an individual's capability to feel free (and as proven by psychologists in the 60's(to many rats living close together creates individual schitzophenic responses and a deterioration in any social structure or community)Ref. Ruch and Zimbardo "Psychology and Life". Second edition

The Individual's social lesson or challenge life has always been that with every FREEDOM there comes a RESPONSIBILITY. And the first RESPONSIBILITY is the RESPECT FOR OTHER'S freedom and rights to privacy. Mature citizenry in this free society is ready for a more deliberative process than our past technology solely based on a representative form of government and deserve it as a survival tool in this age where we need a check and balance on our data acquisition technologies and present use. We do however need fast data acquisition to determine the best use of resource and impacts to better manage this more densely populated world. Therefore, it is fitting that the PFN/TRAC system was deigned to provide accountability to all parties for every interaction and transfer of data to build trust between individuals and demand respect from all individuals in using the system. This is accomplished by giving real-time evidence for any malfeasance and or negligence by identifying equipment and personal identity of the user in all data management procedures and storage. This will assist in deterring hacking and the FACT system should be rapidly produced and placed into service into today's computers and the Internet as soon as possible. There is nothing wrong in the acquisition of information to the most private level of an individual, but it should be kept anonymous transparent, encrypted and not released without the correct constitutional authorizations of the individual and in regards to their right where the rights to compensation for damages must are secured by accountability in the process e.g., PFN/TRAC systems.

True there are many immature individuals basically not ready to participate in a true

real-time democracy and many others are not developed well enough socially and emotionally to allow others to be democratic. The sad thing is that many of them are politically empowered by the antiquated and corrupted process by which we govern our selves today which was the same in the past and will be so in the future as our forefathers recognized. The same human learning curve from being self centered to being able to be social (elitism, Tribal or clan prejudice, political parties, gangs and private interests) are all of the mechanisms used to feel comfortable socially in the past.

Trust and fair play have always been the issue for real fear and paranoia These are very poor forms of public voice and their use of power has deteriorated the individual's right to be a part of the public's voice. In fact today there is no public voice at all, just a lot of private interest people practicing their own body politic and claiming to speak for the public. The PFN/TRAC/FACT system is designed to return to the public free speech and the public voice with real-time accountable polling on issues at the speed of today's Lottos. It seems like a worthy direction to access the real public voice when compared to just a revenue and entertainment device using this kind of technology enhancement. FACT programming will ultimately be apart of every control circuit and many will support interactive terminals, where individuals can identify themselves and participate in deliberative discussions on issues and vote in an accountable manner.

When The United States was an isolated nation in 1776 and small in populous, as well as geographically less connected and influential on each individual do to the vast space and natural resources available for each individual to pursue life and happiness, our representative form of government was less toxic and more easily accessible for correction to an even less diverse populous. And even at that time the injustices were widely and openly committed to block access to decision making in governance (the classic, e.g., Native Americans and the Negro Races)and the pursuit of life and happiness by the narrow minded elitist of that time (all who think they know best for everyone else). This will be an on going process for humanity for all of time as each individual struggles to understand the gift of their life and existence with others here on the blue marble (earth) The learning curve of human behavior to learn social skills presently spans some 80-100years and in to many cases individuals do not ever gain the capability to enjoy the cross sections of other human life they have been blessed to share their existence with. Truly we have to improve our social skills quicker because future survival with a larger populated planet will require cooperation and management of populous and resources or the impacts and lack of resources will kill us and deteriorate the quality of life.

PFN/TRAC systems has been created to perpetuate more individual democracy in

real-time to provide the necessary understanding to a vast many for the role of self governance and greater creative options. Given the responsibility of responsibility of self governance will free humanity to explore possibilities more rapidly including their own individual emotional and social development. PFN/TRAC has been envisioned with the spirit from the great Greek and Roman Democracies, England's MagnaCarta and of course the United States Constitution as the proper present technique to inform the public and poll the public in an efficient manner so that the individual can participate in self governance knowing that their participation will be direct and accountable access to instruct their representatives or to help shape any decisions on any issue of concern. This technology and secure Accountable FACT programs to watch dog any usurping of any voting process constructed by the people is the only real way to insure the first at amendment FREE SPEECH IN THE UNIDED STATES AND AROUND THE WORLD.

IT IS EASY TO PREDICT THAT THE UNITED STATES WILL HAVE THE SAME LIMITED FUTURE AS PAST WORLD POWERS IF WE THINK BEING A SUPER POWER IS OUR ONLY WAY TO SECURE US AND OUR WAY OF LIFE. , e.g., THIS THOUGHT HAS HISTORY'S LESSONS ALL OVER IT - NATZI GERMANY BEING THE MOST EVIDENT.

It matters little what the ideology is Because no matter what it is it MIGHT VERY WELL NOT BE ACCEPTABLE TO OTHERS.

The United State has to continue to offer in it's present technology and way of life exports an improved management and fair play policy to instill trust and a willingness to peacefully cohabitate this earth. The PFN/TRAC/FACT system is faceless and fair and can be a great interactive tool while respecting any nation state's free choice as they deal with free choice at the individual level in their culture and societies.

Figure 23

This Figure is of a personal PFN/TRAC system which can be used in home management control security commercial management and mobile management, however the later is probably not as needed to track personal assets People and Pets because most all mobile PFNS on equipment will have tracking and accountable telemetry. The personal PFNS and tracking devices have been singled out in a later application filed presently as a provisional docket # 112756-700 to better develop the PFN technology commercially and legally as it pertains to society. However some discussion will be done here in Figure 23, 23a, 23b, 23c, 23d, to substantiate with specifications these products and subsequent claims.

Personal PFN/TRAC products can be belts bracelets, articles of clothing and or

personal items either attached or carried by a person, animal or mobile object. The following drawings have been chosen to explain the hardware and detail the types of uses 23 was designed for the conditionally released in society like parolees. This is not the only use or configuration. All of the 23 series drawings are done using a belt configuration, once again this is not the only configuration to these devices

Track a Con.COM This system would allow for parolees to be back in society while their movements and activities were monitored and governed by an automated computer system that would track physical movement through GPS, or LoJack or Cellular and or RF triangulation on a personally carried device that monitors body temperature, pulse rate and provide for positive Identification, e.g., Finger Print or eye iris evaluation
The device would be controlled by the master controller and support local Web page access and hyper-link capability. Tactile and galvanic sensors would be capable of detecting chemical changes in perspiration and determine the chemical equivalent for a specific person drinking and provide a specific electrical signal that is transmitted back to the parole center for a con beep and direction to either report in or take a skin prick check or a breathalyzer. Locations of area liquor dispensing or known drug activities and be plugged in as trail markers on the GPS and flag a convicts questionable activities or ask for the above checks. Prior victims of crimes that an Ex-con is convicted will be notified of the TRACK A CON.COM and the Con will be given a reasonable distance to stay away from the victims. Once again the appropriate trail markers will be posted as GPS, ETC. Geographic coordinates and will notify authorities and victims of flagged improper movements. The convict will be alerted as will and warned to report in and move out of the area. Also the victims can be outfitted with a mobile page and or Track system a warned directly of a past ex-cons close proximity. Additionally the victim and community can track the parolee on the system by contacting the web pages.

2201 is a bracelet or belt to attach the personal PFN or tracking device to a suspect criminal or child or anyone for that matter 2206 is the unit itself with a fingerprint thaw that can insure that the correct person is wearing the unit. The system could have an iris recognition device, pulse sensor galvanic skin sensors, contractor for skin prick or breathalyzer system that can monitor the wearers activities and body reactions. There could be any of the different communicating devices as listed and a processor and memory storage all application specific but basically taken from all the technology contained from all the inventions related patent applications. And the power source could be a battery or the electrical power could be provided by contrasting metal inserted into the body of a human and basically use their body as the power source.

Ultimately an entire micro transmitter system could be place under the skin in another modality with no belt at all.

To continue with the Figure 2302 is the antenna 2303 the antenna lead would be incorporated in the belt. And 2305 is the battery. This is being brought up with a new drawing presently but numerous modalities for this separate invention has been detailed in earlier patent applications. It is important to remember that these monitoring and management systems can be either, ether nets, intranets of any size and or interfaced or operated on the Internet depending on the type and range of the wireless equipment utilized as well as the application desired. 2306 is the personal PFN encasement and application will determine it's configuration and structure. Many security seal systems and security features are detailed in the subsequent 23 series Figures for personal PFNS as well a detailed in other related PFN patent applications. Also inside this containment is the local memory. And 2301 is the belt strapping or band. In later drawings the belt is shown with a security signal wire or bus and preset resistance through signal wires (that can be switched randomly through multiple leads and sensing terminals back in side the containment to prevent shorting and fooling the PFN to think it is still attached to the parolee in this case). Figure 23 shows the use of a PFN with a tight intranet and Internet capability for the victims of the parolee in the past. As later displayed the PFNS will be used for watching children, or for nursing applications, and tracking people or pets in any telemetry application or performing accountable remote control and management activities

Figure 23A

Figure 23a depicts the first of three major different communication modalities. This Figure deals solely with Radio Frequency (RF) equipment connected to GPS equipment and interfaced to modulate NEMA location data strings by modulating, either ASCII, TTL binary coded messages or any communication software over radio frequencies. This diagram depict the modality used in the present the personal PFN prototype. The drawing is general but clear to anyone skilled in the art to recreate this invention for personal tracking. It also should be noted that there are many modalities to achieve this same RF Product but any and all fall within the nature and scope of this detailed invention. Another important note is that these detailed modalities are also used in the Machine messaging modalities applied to vehicle equipment and machines, but these are being detailed here as commercial variations and products as Personal PFNs specifically for people, pets and special assets as defined by the inventor.

Object 23A01 is a two way hand held radio in the case of the prototype it is a small

family channel walkie-talkie operating in the frequency range of 462 mhz-467mhz. The dark line between 23A01(radio) on the left and 23A02 the modem on the right represents a Mic. Line and a Speaker line as well as a signal ground line. These lines connect on the radio to the Mic jack port and the Ear phone jack port and share the same chassis ground which in this case serves as a signal ground. The right end of the mic line connects to a serial input pin labeled TXD for transmitting data and the speaker line connects the RXD for receiving data from the RF component. 23A02 the modem in the present prototype is a Kantronics 1200 RF modem and it has a 9 pin serial connector provided in the standard configuration for receiving and transmitting data as well as supplies a pin for the signal ground the last connection for the right end of the left wire. Then from 23A02 the modem to the laptop or desk top computer N0. 23A03, the line to the right of the modem has a 25 pin connector that goes to a 9pin serial DB connector in the back of the computer #23A03. Because most GPS NEMA protocols run at 4800 baud rate the prototype is set at this rate in the computer 23A03 and uses comport 1. However the RF modem only runs at 1200 baud to transmit and receive over the walkie-talkie so this in the rate of this prototypes system. Down below in this drawing is the belt system and GPS transmission section that sends the mobile location data stream to be tracked on 23A03's computer screen.

23A04 is a second walkie-talkie also having a Mic port and an Ear port set of jacks. This time the Mic TXD line from the radio is connected to a Tigertonics Module 23A05 which is a quarter of the size of the 23A03 modem connected to the computer. This is accomplished with a J11 phone jack the same as used for standard phones and also used in this technologies first vehicle PFN prototype to stop the unauthorized use of a vehicle detailed in earlier related patents. This jack has TXD, RXD and signal ground connections provided through a removable J11 connector. The input side of the Tigertronics module 23A05 has a 9 pin connector that can be connected to a GPS antenna object # 23A06 in the drawing. In the case of the Prototype this is a Garmin 135GPS receiver. However experimentation with Delorme has also been done. All the GPS antennas are not the same and they run different software communication programs in their firmware. For this reason it is important to know if you are working with Binary codes e.g., Rockwell serial or ASCII or TTL or reversed TTL in choosing the modulator 23A05 and the Modem 23A02 as well as the proper software programs to the GPS data. at the application level for the calibrated Bit maps on the computer 23A03. The hardware connection from 23A05 to GPS 23A06 must support the functions necessary to satisfy the GPS 23A06 receiver protocol for transmitting as well either with the DTR Data terminal Ready of the RTS ready to send signal as well as support the TXD and Signal Ground.

NOTE: Product hardware consolidations will combine the part 23A06 GPS receiver with the modulator and or demodulator circuits 23A05 and the radio transceiver 23A04 in one board in it's tightest configuration with special consideration to the RF antenna and GPS antenna for interfering with each others performance for the personal tracking belt and system.

For the monitoring function the modem circuit or demodulator 23A02 will be on the same IC with 23A01 the radio transceiver or receiver component. This system can also have a AC power cube /DC converter for 6–9vdc to either charge the radio/demodulator unit or just power it. However this system would either have it's own power source or be able to receive power from the power pin on the DB9 connection on a laptop for mobile movements.

To reduce cost further this product for personal tracking only has to communicate in one direction. Which means the personal tracking portion on the belt need only a transmitter and a modulator with a GPS receiver, and the monitor portion only need a compatible demodulator and radio receiver with the interfaced computer and viewing monitor.

Before returning to the computer software to run the tracking function with these connected hardware products and components a moment must be taken to explain the power systems on the belt.

Power is provided by either a rechargeable battery pack on the belt for the mobile operation with (accessory solar cell strips with velcrove stick-ons for hat or shoulder pad mounts that plug into the belt power pack. A temperature sensor on the battery packs disconnects the solar cells if they reach 109F (experimental charge regulator process for Ni Cads, Lithium, and Alkaline. Temps for safe charge not equated at the time of this provisional). Power first enters the modulator23A05 the passes though the power switch and fuse and then enters the modulators voltage regulator circuit and is passed out pin 9 on a standard DB9 serial pin to energize the GPS receiver. Battery ground exit Pin 7 to the GPS receiver completes modem and GPS power requirement with additional 5 volt regulator installed to adjust power to energize the hand held radio unit that is interfaced as the transceiver. This basically is the prototype at the present time, however in the products to follow all sorts of telemetry is possible, as well as, providing accountable remote control and management though the two way communication and memory storage components. Other components on the belt system will provide a locking clasp and security line that detects the real-time removal of the belt or tampering and reports and records this activity for authorized conditional freedoms etc.

Returning to Figure one to discuss the software used to create this feasibility prototype. The software running 23A03 the computer to utilize the NEMA GPS location

Data generated and received thus far are as follows. The initial software to handle the RF modems software NEMA code data is the Automatic Position Report System (APRS) software shareware protocol. This program converts the received data into GPS coordinates to generate and object on a calibrated map. For the Prototype the Delorme 6 edition of Street Atlas is employed however maps can be created and calibrated as a library file and the APRS software will pace the tracked object on those Map. These two base programs place the object on the map but in most cases the overlay default map in these commercial products is to general and they do not support a continual zoomed in view on the personal belt location, when combined with this APRS share ware needed to update the small movement of an individual walking etc.

The zoom feature serves a most necessary purpose and function of these personally worn locating products, which is to instantly and continually acclimate the viewer to the area. To accomplish this a third piece of software was required to make this a great product. The objective was to zoom in on each update and hold the zoomed in position in the center of the computer screen and repeat this process at each update (timed at 9 seconds for the prototype - but adjustable). The present prototype zooms in from a approximately 7mi radius to an area of less than.1/2 block. This is accomplished by using a Macro and keying the computer key board function to zoom at the desired time to the most detailed bit map in the library. Of course a zoom out to a national view is equally obtained if so desired

Kline and Walker LLC in the development of these products will work directly with the calibrated map companies like Delorme, Garmin, Fagawi, Tiger maps and or any government mapping programs etc. to accomplish these functions and make these personal PFN commercial products more user friendly for the general public. These functions will be easier to create through the proprietary software commands after knowing with the correct software codes. This is the main modality to make these products user friendly.

Once again, this is not the only modality to create a personal RF PFN/TRACking System and any number of frequencies can be utilized through this present modality and many are named in this technologies prior related patents. But this is an easy to understand way to create a feasibility prototype of this invention to perform inexpensive short range personal telemetry of an individual or pet's movements. It also supports all the feasibility necessary to prove this technology as a personal PFN system for all the detailed communication modalities.

Additionally this range can be increased by different radio systems, repeating or digitpeating though other radio stations such as amateur radio or ham operators, or by repeating through other PFNS either equipment PFNS or these personal PFNS that can pick

up transmissions through programmed scanning capability or by programmed digital transmissions which respond to emergency protocols or digitpeated commands as a transmission string. This software is running in the APRS shareware program. Additionally, the hardware consolidation into an integrated circuit configuration for these interfaced components or devices is a regular activity for anyone skilled in the art of reducing and drawing up IC boards for radio frequency equipment. Meaning any product resulting from this inherent described and predicted process is all with in the scope of the PFN invention and should not be considered unique, therefor falling within the nature and scope claim of this invention.

Note: From the first description of using short range RF systems in PFNs a repeater function has been detailed and described as a major function for providing long range capability out of small radio transceivers. In all the prototypes in this application short range RF systems are employing the 2 way family radio frequencies of 462. Mhz and 467. Mhz. These are by no means expected to be the only frequencies for these applications. All of the applications will have to receive government approval from the countries governing agencies such as the FCC here in the United States.

Figure 23B

The next two drawings Figure 2 and Figure 2A are first a new drawing detailing the two way paging systems(fig 2) and also 2A the previous depiction of two way paging and GPS system for personal movement use. They are being shown together in this applications to substantiate the earlier filing of the idea and to bring all these personal tracking and PFN devices in to on area for commercial development. Both the old and the new drawings and descriptions will be covered in this pager section.

In Figure 23b on the left side is a computer either a Laptop or a desk top computer with three numbers on the left side. The numbers are 2301b, 2302b, and 2303b. These show the possible commercialized products that can be provided from a pager locating system. In this pager locating modality a GPS receiver is likewise utilized. But also the pagers locating system a signal triangulation algorithm in the system software

Note: So the use of a cellular phone or paging service software running a triangulation algorithm using the fixed position of the towers for cellular phones and or two way pagers, to locate a specific transmitting pager, phone or combination device's position in relation to the known position of the towers.

This technology is claiming this technique to locate a specific two way pager's transmission signal as an alternative locating modality for both types of PFNs (for people and

equipment units). This system will save space by removing the need for GPS in many cases where service is good and the need for a large battery. This will be a much improved modality for this innovative locating device in the future which will be provided as a product improvement by inheritance for this technology. Kline Walker LLC will strive to develop this tracking modality (Systemically) with companies like Nextel, Motorola, Bell Atlantic and other pager companies, who are developing larger short radio messaging tower networks and multi-communication systems and devices. This has been explicitly stated here and now as an other modality for this same personalized tracking device or PFN and is considered with in the nature and scope of this invention in any evolutionary form.

Returning to Figure 2, 2301b on the computer is a commercial web site that supports maps and tracking service most probably provided by the paging service. By using the paging unit's ESN from the paging service's system software the (two way radio, or wireless telephony) would generate useable earth coordinate data obtained by distance and directional sensing equipment or functions performed by the receiving tower hardware and firmware and send this data to a paging system software via paging system software protocols, which during the process of the signal employs an automated triangulation software algorithm based on known receiving towers fixed positions on the earth to provide at least an accurate two dimensional fix of longitude and latitude to be applied to a bit map or calibrated map program to be run as a web page, personal E-mail shared providers cable or Satellite (joint ventures with pager provider) or run on an individual e mail site through the persons Internet provider with/ IP protocols and application specific software (possible joint venture Internet provider and Pager provider)at the application level with all data transparent till the end user inputs user ID code Pin number password to bring up the tracking and location telemetry on the bit map on a computer monitor or other viewing connectable device e.g., PFN assets as detailed through out this and the related filings.

Or as they received pager message packets transmitted into the system the messages would carry NEMA or GPS data in some format from a connectable GPS receiver that is interfaced to a two way pager (processing separate or as part of an integrated circuit), which when activated would allow the service software to pull up the correct calibrated bit map and pace the identified paging unit etc. as an identifiable Icon, number, symbol etc. to the computer viewer, when they entered the correct pin ID upon entering the web site as the correct authorized subscriber to the service. 2302b represents the same process operated by government agencies, for conditional released of convicts or parolees. This application would allow the judicial and law enforcement to monitor restraining orders in real time along with dispatch medical staff and perform interdictor functions if need be. This technology is

detailed in Figure 9. Also, victims can be given alert reports and visual updates, by automated Page messaging, Email, and telephone messaging embedded in the software command structure to be entered by the authorities. And the Government can defray another program to cut health care cost by providing this service to the economically destitute in need of a watchful eye for the mentally handicap those with dementia, Alzheimer's suffers or the severely physically handicap where expensive nursing service can be either reduced in cost and made better from professional or a family member. More freedom can be given to the health care provider because they can monitor a disabled patient or love one in one location including vital signs while doing other activities near by. Drug firms and Insurance companies could sponsor these web site inexpensively or free with other advertisements running to pick up the cost. 2303b can be a personal e-mail address where the individual has purchased the software to run on their personal equipment making it an intranet at the very least. And of course they would be capable of sharing this tracking with other agreed upon email web sites. Much of the technology has been detailed for this in the Radio frequency modality in Figure one, however there is some other modalities possible to achieve this for all three of these configurations and product offerings 2301b, 2302b, 2303b. One of the simplest hardware configurations employs a GPS receiver 2306b (Garmin, Delorme Lassen, Rockwell Jupiter etc. or a chip set and antenna Philips, Motorola etc. with the appropriate op amps and connectable interface with a processor (Stamp computer) that is programmed to condition the NEMA signal into a packet of characters for the pager protocol and interface with the two way pager and send the command to the pager device 2305b to transmit the GPS NEMA data packet in pager protocol to the paging service that has the software command to complete the programs described above. This of course is done by using a developer program from the paging service to interface with their protocols. Once again Kline Walker LLC has detailed this out as a commercial undertaking with a number of companies because of geographic dominance in the market place. First contact will be with Motorola's flex and reflex protocol companies in the United States and with RIM pagers in the Canada. Nextel also does short radio messaging in both Canada and the U.S. In Europe and the European Radio Messaging System ERMS Phillips and Erricson etc. . These companies and commercial plans are being stated to increase understanding and cooperation to achieve a working relationship with these manufactures to develop the entire PFN system.

So the RIM pager systems and the Motorola page writer 2000 are two units that supply access port to send messaging through the pagers transmitter so long as the data is in a format that the pager protocol require to handle that data. other systems than the Flex and reflex Motorol paging systems have also been detailed in the earlier related patent application.

So many other variations to interface with pager technology have been detailed previously. However with paging manufacturing providing the physical connectable systems and interface protocols for the combination with any 2 way paging and GPS as well as two way telemetry have been made far easier than before and much more likely that they will be part of additional multi communication devices serve this technology's PFN's effort to act as an organizational interface platform that provides accountability for all sorts of activity controls and sensors as has been detailed in earlier related patents and exemplified here for telemetry data(NEMA) in tracking. Obviously A private intranet could be created with a calibrated software map libray on a personal Email address equipped with the software program that processed the NEMA or text data delivered through the paging protocol to the Email address and place the tow way pager's location on the proper calibrated map for the solo user or small business user. Thus two way paging with GPS is another viable means for Personal PFN/TRACking or for the Machine messaging PFN's. Along with cellular and pager automated triangulation protocols (product construction and commercial arrangements will determine locating technology employed in this technology's personal tracking devices or PFNS

2304b in Figure 23b is another paging device capable of receiving direct two way paging and this device supports an LCD display and firmware for displaying tracking to display another remote location two way pagers location as well as it's own position from it's GPS connection or if a pager system is running triangulation algorithm to provide location from tower distances rather than GPS.

Returning to the drawing as a RIM pager 2305b, specifically a IP-950 pager is employed in case a Trimble Lassen SK8 GPS will be used as the GPS receiver. Through the CommRegisterNotifyPattern feature of the pager the serial port will be closed and being charged through the PFN processor running this firmware. The PFN processor will be connected to pin 2 DTR output and pin 4 DSR in put of the IP950 pager. There is already a protocol written for the software commands between a processor, Rim pager and GPS receiver in the appendix of this application, which was down loaded off the Internet from WWW.fleetcommunications.com. However the pager 2305b interface communication in this modality to the GPS 2306b is through TXD_A and RXD_A under TSIP/normal RS-232 for TAIP or other protocols. In this case the serial port communications take place at 9600 baud, 8bit data No parity stop-bit 1(9600,8 N,1)

The default protocol will be TAIP format. All hardware terminals and contacts as well as software commands and protocols are in Appendix I. Other two way paging products and protocols for locating systems through Motorola products like Page Writer 2000™,

Create a Link II™, etc., have been detailed in related PFN patent applications 2308b in Figure two is the belt 2309b is the power pack 2310b is the clasp for the belt and 2311b is the security line and or antenna which is completely detailed in Figure 23E. Figure 23E will detail all the specifics for the personal tracking PFN system and all the hardware connections. The belt bracelet collar or clasp system is in no way the only modality for the personal PFN to be deployed on an individual or and animal.

It may take the form of a concealed device in a garment or actually be surgically implanted in an individual or animal and powered though contrasting metals that would create a potential in the body fluids making the body a battery or have a power supply much the same as a pacemaker or an automated internal PAC or medication dispensing device. These modalities were discussed in earlier writings and details as to the protocols and specific actuators for these personal PFNs will be entered into any open PFN patent application for the technical specifications however, any and all actuators linear of rotational compete or fractional have been detailed so that anyone skilled in the art can readily construct any application specific actuator control it and energize it. Of course internal PFN implants, (Transponders) have to be small in size low in current demands, so actuators would be constructed from small actuators or MIMS micro machines as small as lice. And created at the nuclear labs at los Alomos. However, the same engineering for liner and rotational actuator applications for normal size electrically controlled devices would be employed. And obviously they would be constructed and placed with medical experts.

Figure 23B1

This Figure is taken from an earlier related patent application and it is being entered here to use the Figure and description to better detail the invention and to isolate out for commercialization the personal PFN and tracking system for people and pets.

Note: 14 series numbers are used from the earlier application for two reasons first because this application does not use 14 numbers for the 14th Figure and it is consistent with the earlier parallel development of personal PFNS and equipment PFNS

1401 is a belt buckle that has a special key to release the locked buckle or electronic lock or any kind of locking mechanism. 1402 is a hard nylon or similar plastic flexible strap resistant to cutting in the most practical way, that has and inner liner of nylon strap so that one or two way pagers and or a G.P.S. system like Motorola "Oncore"XT, XTsII,GT, UT, VP or Philips G.P.S. chip set mentioned earlier in this application can be secure and concealed in an protected enclosure between the two nylon straps to store these G.P.S. components along with differing levels of transmitting devices that can receive signals or messages, transmit signal or

messages, and or alert of sound alarms on both sides of these transmissions.

This 23b1 is Figure also 14 from an earlier PCT and U.S. filing for this PFN technology

Figure 14 displays varying levels of one way and two way pagers and C.O.T.S. paging protocols as well as voice paging applications. However, as earlier mentioned; this invention provides for short RF signal transmitters with their transmissions received by every piece of equipment that has a PFN. and will ultimately all have RF transceivers to receive these emergency priority signals and condition the signals and repeat them in a pre programmed manner over what ever long distance communication hardware that exists in the PFN to the proper authorities. This is a repeater function deserving of special consideration and is not the same technology stated hear for the pagers in Figure 14. As has been described and maintained through out all these applications. However, these types of carrying systems, e.g., belt or bracelet or even clip or tape on systems and the qualities, properties and capabilities claimed and demonstrated for Figure 14 are the same as claimed for the repeater technology as well. (Note: this Figure description is from an earlier patent application and is referring to repeater Rf systems and PFNs as mobile stations. For personal PFNs)

And while they can perform many of the same tasks they are two distinctly different technologies, and are herein so stated, however equally protected in this and the related patent applications.

The G.P.S. chip set or IC board is represented in Figure 23B1 by #1405. 1407 is the patch antenna for the G.P.S. and this cable would be place into the belt and follow the contour of the belt to be concealed. 1403 is an extra battery in some equipment variations and a way to give longevity to the entire locator belts functions. 1406 is a speaker or a loud speaker if a monitoring protocol determines it to be the best option to send a message either via a pager or cell phone signal, e.g., Motorola reflex protocol to alert the person wearing the belt, e.g. , criminal leaving a restricted area, or child lost and a public announcement is desired to seek aid from responsible adults in the area. The speaker could also emit a loud electronic whistle or shrill alarm intermittently to attract attention to the wearer of the locator belt or band.

All of this would be initiated from a remote phone page or cell phone call. Some of the C.O.T.S. Pager products that will be used in the proto types are the Creatalink pager processor both one way and two way, the standard one way and two way pagers (reflex protocols) using the interface technology detailed in earlier related patents, e.g.,current sensing as was done in the first patent and Binary/ASCII/NMEA BIN/Loran from the G.P.S. all processed into 20 bit data segments to meet the Motorola reflex protocols for transmitting return data. Either through soldered connections, or BNC connector DB9 for RS232 as

already detailed. The software for these applications are available for product development for this product through Motorola and only the specific software commands must be written to create the desired functions. This is easily accomplished on the PC and downloaded into the chip set processors.

This is the case for all the interfaces described in these application and due to the many different types of combinations to achieve even this simple locator belt it is not practical to write the exact programs and in fact is much more clear to describe the functions verbally or with flow charts and list all the hardware parts and software components available for even the unskilled to write programs. Anyone skilled in the art and even a hobbyist who can read will be able to buy these parts and the software packages and write these basic controller programs in a matter of hours. This is why the functions are focused on rather than any specific basic programming command string.

1408 is a voice recording chip to give prerecorded messages as triggered from phone pages as described in the first related application for the stop and control box. 1415 is a processor if the Creatalink is not used and it could be a small stamp computer. A Stamp Ior II; although Motorola and Philips as well as Siemens Tech, Radio Shack and a host of others all make micro controllers or processors to turn on the voice chip and speaker or hailer when they receive and recognize a coded message from 1404. Or if the water sensor sends a signal (the small square [W} in 1408 indicates a water sensor which would go off if the wearer of the belt was being submerged in water. And Of course all the electronic equipment is made water proof.

1404a shows a C.O.T.S. standard one way pager with the inventions proprietary non intrusive battery peg 1409 connected to a current sensor chip exactly the same as the first patent for the stop and control box to sense a silent pager vibration activation. The chip is connected to the voice recorder chip so when a phone page is received it draws current down out of the battery peg circuit and creates a ground on one pin of the current sensor which triggers the voice recorder or howler or hailer through speaker 1406a message or noise. And or a small micro controller with a EEPROM can run firmware programs to alert the surrounding public or in a two-way pager reflex protocol application monitor 20 character bit audio sound bite of what the wearer is experiencing. And the power is supplied by the battery 1403a in the in the recording system. These systems could also use the same system as the PFN.'s and record the surroundings or report back sound and or data.. So with special monitoring equipment on hand these pager locator belt systems could call in if someone had a medical emergency or hit a panic button.

1402 is a belt on a man walking on earth. 1410 shows 4 satellite a minimum for

getting G.P.S. coordinates and most systems mentioned use at least 6 satellites and as much as 8 channels are available for taking a reading in all the Motorola chip sets. 1411 (SG) tower is a commercial server or land line phone node or gateway as has already been thoroughly described. 1411 tower will pick up the page signal or RF signal or Cellular system, if these technologies are employed and convert them through phone modem and transmit that signal down a ISDN phone line or comparable to at least one computer 1412 that is running a G.P.S. program to monitor the Bin/ASCII/NMEA earth coordinates and time coordinates data transmitted to 1411. Also as was described earlier the coordinates could be monitored from the car 1413 if the car was the phone data node or the car was able to network with 1412 to receive down loads for the data of earth coordinates. All easily accomplished as described earlier. The second Figure down in upper left is the belly belt locator belt laid out flat. And 1401 is the lock buckle 1403 extra battery 1404 is the pager 1405 G.P.S. 1406 speaker or hailer or howler. (This description of Figure 14 relies a lot on the detailed technology of the entire earlier patent for the equipment PFNs so in reading this description remember it is necessary to read all the specific modalities being detailed in this application for pagers, RF equipment and Wireless phones. The drawing and concept are the main points of this Figure and that the personal tracking device or personal PFN was an early parallel development with these varied communication systems and locating equipment as well as varied configurations detailed earlier as consolidations of devices into muti-tasking equipment arrays involving Telephony and location equipment including such product as mobile office units, which were designed to plug program and play with the equipment PFNs)

Figure 23C

This Figure is the basic cellular tracking system that has always been a part of the earlier related patents in uses the PCMCIA Complete Card ™ which is 2305C in Figure 23C (RIM also makes a comparable PCMCIA card with a cellular transmitter, a 386 processor for the modem and an antenna) The PFN technology has been detailed through out the related patents for anyone skilled in the art to construct each C.O.T.S. component that is used to create the feasibility prototypes. But additionally a crucial component and quality of this PFN technology is to be constructed to be user friendly and produce an accountable electrical interface platform of plug, program and play user friendly forward, present and backward engineering capacity to accommodate a large variety of devices and achieve as universal interface as much as possible.

So either of these cellular modem transceivers will function well for this variation of the personal tracking belt or device. There is also a myriad of newer cellular modems coming

on the market everyday and some have protocols that provide programming for DTMF functions or automatic dialing. However this invention was also designed with an additional mini computer 2307c which would perform the preprogrammed dial up functions to report the GPS 2306c data to a phone line connected 2304c or wireless connected 2302c. 2307c will have local memory to perform accountability for activity controls communication and the verification of data reported for complete personal PFN functions 2306c is the GPS receiver which in some cases will be connected directly to the RXD and RXT as well DTR RST terminals in the PCMCIA card connector and the proper electrical connection to energize the card to the battery 2308c. Many battery pack and charging systems have been detailed in this application and the related patents and will be by passed in this discussion presently as obvious to anyone skilled in the art and as inherited from one communication modality to another as detailed earlier. 2309 the belt and 2310c the belt clasp either locking or not (this will be described in Figure 23E).Of course if the mini computer is in the loop then their would be software to process the incoming data from the GPS and outputting it to the cellular modem and calling the correct number. Once again if a software protocol and standard is being used by telephony company systems many of these communication functions will be handled there including IP protocols and final application programming to display tracking or report other reported data streams. These protocols have been named and the developer programs have been named. But as welcome as these advancing phone technologies are to the PFN system they have been predicted and described as consolidations of communication and processing in all the related PFN patent applications and still fall within the nature and scope of the invention when employed for these purposes of accounting, locating remote management and control. Garmin came out with a a GPS Phone recently that when coupled to an other companies software can track the phones location though polling the GPS phone through call to receiver dial tone response to perform a look up function on fagawi software and maps that are calibrated and will correlate the tones to latitude and longitude which relate to a specific bit on the map. These of course originate from the Garmin GPS receiver in the Cellular phone and are processed from NEMA data or Binary code ASCII or HEX to the dial tone sounds in a micro processor with this burned in firmware then they are transmitted over the phone where they are recovered with the Fagawi software operating with of course an IP phone connection modem and computer plus monitor. This is two companies selling two products that can be put together to perform this function and this technology has been described in the PFN'S earlier patent applications and is considered another prior modality to be used with analog cellular phone RF and Pager systems to send data DTMF of any type wireless. For this technology of course the limitation is speed and the amount of data but it is

suitable for tracking. This system has been used basically for analog signals and PFNS will be capable of interfacing these systems.

The real need of the PFN requires digital communications for efficient data handling. Presently most all the wireless communications are being converted to digital DMTD or CMTD for the major phone providers. This of course provides greater security, which is the main reason for the change. This security is needed for the PFN functions as well. The next drawing is a detailed consolidation of communication systems involving two way radios, telephones, and paging systems in one wireless phone system Nextel.

This is a described combination of communication systems through out all the PFN related patent applications and fits right into the multi-communication array and plug, program and play capacity as a consolidated improvement

INTERNATIONAL COMPONENT NOTE:

Research In Motion Ltd. RIM is a company in Ontario Canada and the manufacture of wireless communication components that can be utilized as an other modality in constructing this invention the either the personal PFN and or the equipment PFN. Even though some of their components have already been detailed in earlier communication modalities, e.g.,RIM Pager-IP(Internet Protocol 950 for pager tracking in Figure 2's description they like Nextel have many of the communication capabilities to provide either singular communication components or a combined array in the PFN. Plus they have different market concentrations and slightly different product quality offerings in their respective markets.

Before entering the combined communication array of Nextel and it's modality in the PFN technology a close look at Rim's OEM Radio-Modems prove to provide some other components for yet another modality to perform all in one cellular, processor interfacing that can support GPS or data streams to be handled as Telephony gateways to IP computer monitoring for tracking by placing mobile GPS/Nema data objects on a calibrated map. Through a tracking software program either running in the computer or a system software transmitting data to an individuals computer or even an other wireless Ip device. Once again just by running a triangulation algorithm that factored the reception towers position in the providers software rather than to have a GPS component with it's additional size, power requirements and difficulties in receiving in buildings, makes this tranagulation system software technology have some very important attributes that can be a great improvement or enhanced in any product offering for these PFNs. Especially the personal PFNS or personal remote tracking devices. Or in conjunction with GPS provide a ground signal component to

the inaccurate commercial version of GPS in PFN applications that will require pinpoint location accuracy in 3 dimensional tracking (much like the 4th earth reference signal used for military accuracy with GPS to adjust for the ionosphere deflection of the satellite signals sent to the earth bound GPS receiver units. This is accomplished with through a software algorithm using both sources of location data and (fuzzy logic). This system will be used to acurately guide vehicles on the roads with other sensors communication functions and video imaging as has been detailed in earlier equipment PFNS.

Returning to the Rim high performance RF transceivers. And the first point is that these could be used to provide Radio close circuit systems at an approved frequency and in embedded in a system as described in Figure 1 to give great range to a close circuit system with 2 watts of power to the antenna in essence these units would replace 23A01 and 23A02 and 23A04and 23A05 as two combined radio/modems on either end of the communication between the GPS unit and the computer from bottom to top in Figure 1. Of course the software and firmware configurations would be essentially the same and there would not be any reliance on towers in general. However this also could be a possibility.

The main purpose in naming these Rim Radio Modems 902M and 801D and 802D RIM Radio Modems is that they are operating on 900mhz and 800 mhz and function through basically cellular or radio messaging frequencies and protocols used by the wireless telephony industry companies and their provided IP gateways. This of course is another communication option for the multi-communication array capability of PFNs in general.

For this reason Kline and Walker LLC will seek to develop this inventions products. That will employ these components through the modalities in this application and the related application in the respective geographic market areas. This would include in Canada Research In Motion LTD, The owners and operators of Mobitex packet-switched narrow band n s t work, which is designed for wide-area wireless data communications. The operators or service providers would include, BellSouth Wireless data in the U.S. Bell Mobility in Canada. Also for the 800MHZ RIM's 801D and 802D where DataTAC® is the narrow band wide area wireless communication network. Kline and Walker LLC would seek in the commercialization of this PFN invention ARDIS in the U.S. and Bell Mobility in Canada. Others would be sot in other international markets like Asia Australia and Europe as they employ DataTAC® or Mobtex or a compatible packet radio software for these frequencies or one those wireless systems so designated by the governing authorities.

It is important to remember that much of the PFN system is designed as a data acquisition system, as well as, an accountable remote management and control system that's primary objective is to aide in the responsible use of resources and equipment both

environmentally and economically for all societies in a fair manner. This is why the use of various manufactures in their areas of market dominance are named and indicated as part of the PFNS technology business plan and market strategy. Also and especially, for the equipment use PFNS Kline and Walker LLC will seek out the World Bank and the International Monetary Fund to aid in addressing economic and environmental impact issues with the use of this PFN technology. The PFN system was created to prepare accurate data for the public and private interests groups to review in real -time so that the most cost effective beneficial decisions based on real data, education, deliberation that result in an all points bottom line reality check presentation can be used in making proficient commercial, environmental and social decisions, regarding investments and projects so that the cost of negative public opinion is reduced, while encouraging private, and public investment and understanding in the process that is presently receiving poor public review. Ideally the PFN system will reduce time, money and resource waste on policy that is clearly un-beneficial or even corrupt and badly in need of public trust; and conversely help to educate all to support those worthy pursuits that are beneficial and develop a better quality of life, an economic tool to relieve social tension for a peaceful coexistence. The PFN factor can become an accurate economic tool for appraising any financial endeavor or investment made by any Company, Government, Bank, or project, etc., especially the equipment and environmental PFNS detailed in the earlier related filings. The PFN system could be a condition of securing investment funds. This accountable data acquisition tool can aid to provide financial stableness to the investment process including the stock market.

Definitely, when used by responsible individuals in a free and fair world the PFN system can be an optimum tool to develop trust, and a quality life as is so greatly needed in this populated earth where population management, environment and resources fairly and efficiently balanced for humanity to be supported in it's physical existence.

Figure 23D

Motorola's Nextel systems as combined C.O.T.S. products

Integrated Digital Enhanced Network service (iDEN)®

Combined digital Cellular with Motorola's Nextel Direct Connect® a digital 2 way radio for instant private and group conversations and text numeric paging in a single phone This system has greater security for communication data. As a primary communication device in both the personal and the machine messaging PFN's these Nextel and Motorola protocols will be a good step in interfacing and organizing C.O.T.S. communication products in PFN's (both personal and for the machine messaging systems)

The Nextel Direct Connect® system operates like a two way radio through the system routing function deciphering digital message headers of preprogrammed ESN address and quickly routing a communication link to the correct hand held unit or units. This technology will function well to create intranets for machine messaging in the PFNs involving machines, vehicle and equipment and for personal PFNs, such as the ones detailed in this patent application and the related patent applications

However, due to Nextel's use of a limited range of carrier frequency for all their functions, most communication systems in PFNs will still require a transceiver unit with scanning capability and function covering at least some other specific radio frequencies (emergency channels etc.) pager frequencies, and cellular phone frequencies (that have emergency protocols that will be handled by the PFN processor or have software or burnt in firmware (for repeater functions or digitpeating signals) in a combined communication device constructed in the future. When these combined communication functions and locating systems are consolidated and integrated to perform accountable messaging they fall within the nature and scope claim of this PFN technology and are also claimed as C.O.T.S. interface products which have been described in earlier related patents prior to these latest Nextel phones products e.g., (i500 plus™,i700plus™, i1000plus™

Shot Message service SMS paging in a PFN when interfaced with the PFN is one modality to provide one and two way paging to any PFN, and as part of a Nextel product offering secure cellular digital phone service and simulated two way direct Radio protocols a most Ideal way to perform accountable remote control and management. These systems are conserving space in the PFN. And with an additional memory function available to the paged messages in Nextel's SMS this could act as a local memory loop required in the PFN for accountability. Of course, the entire phone or this memory function part would have to be contained in a protected area physically and electronically from tampering. Also, the web page control system could utilize Nextel software to send a remote control page to a PFN either personal or to an attached piece of equipment to perform an accountable remote activity and record that command in the system buffer(Mass data Storage System) as well as an local memory supported in the PFN. Then other software Macros can be written and employed to key stroke commands in these running software programs on web pages to further automate the process, or by knowing the appropriate key code for the software program enter the commands to become an operating component of the running communication software program. Of course for PFN mobile tracking any of the communication systems can be employed to send any NEMA/GPS data back to a personal web site so long as the software is appropriate at the application level to place the coordinate data with the right identification

data as an object on a calibrated map on a computer screen, monitor or interfaced TV with Video Game Map Program. Or processed by commercial TV server boxes. (This is a new concept for a cheap product for those that do not have a computer.) (a video game software program that is a calibrated map program and could be hooked to an RF modem interface w/proper connector, or inexpensive phone modem interface, to receive the Personal PFN's locating data and place the located object position on the correct map on a regular house hold TV or this service can be offered by the cable and satellite TV people in conjunction with cellular phone and pager servers through communication links (IP, etc.) that routes to the subscribed recognized PFN ESN signal with NEMA GPS or any location data. The PFN/ESN signal is ID by the communication device being served (may also carry PFN/sn) then the communication server sends the data stream to the subscribers cable, satellite, or computer provider or web site or E-Mail address (as directed by an accompanying command communication string that is created by the subscriber at the time of acquiring the service – this is entered into the systems operational software so that the location data (or any other telemetry) becomes available to the account holder or their authorized persons, when accessed by a specific pin number or security code, which will unlock the transparent data or encryption in the final application software (either local or systemic run) for these end users to view location and see any data telemetry from their mobile PFN asset. Either on their regular TV, or computer monitor (other such viewing devices may include wired or wireless lap tops, palm tops, organizers, GPS handheld units with communication capability, Cellular or wireless phones or pagers with displays and appropriate tracking software named here as separate personal PFN technology devices and variations, or displayed by a PFN system equipment or personal version). These descriptions have been detailed as a PFN priority system for tracking assets inexpensively for people, pets and their personal objects involving and employing a variety of devices. It applies to both the personal PFNs and the machine, vehicles and equipment PFNs. It can be operated as an intranet on limited RF equipment for limited distances or it can be a limited intranet through repeating or digitpeating through other PFNs as relay stations. Or, it can be a closed circuit intranet by IP protocols and proprietary protocols detailed above till the data reaches the subscriber at the application level, where personally owned and operated with a phone modem computer and software. Or the subscriber can authorize their communication provider to route their personal tracking or PFN telemetry for any data through an IP gateway to the Internet via commercial private, public(Gov. or Non Profit gateways) or, the in house communication provider's IP gateway link can be the route for sending the data to a common company owned web site for general viewing. Or subscribers personal e-mail wear the Internet provider supplies the posting

software to convert the signal to display the telemetry data through the correct software and viewing screen architecture for, e.g., tracking (maps), physical telemetry (graphs heart rate, BP, etc.), multimedia, video, audio etc.) (windows based, etc.). Or servers sponsoring advertisements can provide this service for a nominal fee, either with individual security (transparent and encrypted, etc. which displays individual views of subscriber assets, or as a mass posting with zoom in clarity on a subscribers particular asset that was made as a personal request to see location (by clicking on) – (all willing responders presently being displayed could be viewed or cleared from the screen by viewer preference).

NOTE: All transmitting devices for 911 protocols such as emergency systems manned or automated, would possess this application level software in their system to process or view all transmitting devices or to activate their FACT public service section to route repeating or digitpeated PFNS in an emergency application. These tracking or telemetry subscriber services functions are preprogrammed with the ESN communication number, PFN SN, etc. to be used in a transmission header (transparent digital binary code, etc.). And also preprogrammed is some form of personal identity check for authorized users of the system and function like PIN numbers, etc., all of which is submitted and programmed at the time of application during the service purchase. This is where the communication command strings are entered to create this PFN network communication and information technology, ideally handled by accountable PFNS, because of remote and systemic redundant memory storage for catching fraud and hacker criminals, with anti-social immature and irresponsible behavior.

These two above proprietary tracking system were detailed here as a set of product lines that can be accomplished though the web using GPS or wireless Cellular (or RF or Pager) automated triangulation to derive location coordinates. And it is a good initiation set of products for co –development with Motorola or Nextel, etc. to be a part of developing this technology to provide accountable PFNs for personal and machine use world wide for better management of equipment time, environmental resources and the control of waste from the individual to the largest corporations, banks and governments. Kline and Walker LLC will be seeking out Nextel Developers Program in an effort to work collaboratively in this above development. Also many feasibility components are Motorola parts.

Figure 23D

This drawing shows multi communication systems interfaced, which is one major organizational function of the PFNS. So the drawing incorporates Nextel's present technology and protocols as another Commercial Off The Shelf (C.O.T.S.) Product for multi – tasking communication in the two different categories of PFNS; Personal or Equipment

PFNs. It is not a panacia or optimum multi-communications service for the PFN protocol, but it is a step in the correct direction to offer a organized accountable scanning function for dedicated RF, wireless telephony, and paging systems designed for PFN protocols. Plug, Program and Play consideration will of course be designed into all PFNS to utilize the Nextel system and Kline Walker LLC will seek to construct PFN product and protocols with Nextel and the prior mother Motorola to provide the PFN convergence scanning devices and system for a multi- communication platform in the PFN along with the FCC (other related government agencies) and standards committees to assign frequencies and protocols for a communication convergence emergency cellular network (a PFN system protocol and part of the TRAC/FACT program functions detailed in earlier related filings). Figure 23 is an earlier patent application Figure detailing the convergence of paging radio and telephony wireless in the PFNS.

The top half of the Figure details the use of computers, and or TVs as everyday monitoring systems to operate personal tracking in the least expensive manner and to add product to this technologies base systems and grow sophisticated accountable personal PFN for remote management and control. This is done to provide product to all economic levels and systems that can be built on as one has the capability or need to do so.

23D01 is a home based PC either lap top or desk top model. And 23D02 is a regular house TV. 23D01 is connected to an standard land line phone in 23D13 through an internal computer phone modem and is capable of receiving any telemetry data from a personal PFN GPS tracking along with other data streams though Internet protocols interfaced with varying types of Internet gateways basically Packetized RF, Paging, cellular phones or wireless phones analog or digital systems CMDT and DMDT by operational software products provided by service providers and prepared for Internet protocols (IP). These personal PFN products and personal tracking products will be constructed in conjunction with Nextel, Motorola, Research In Motion LTD and will range from recreational tracking and hobbyist devices on isolated systems to serious accountable systems connected to intranets and the Internet initially starting with tracking functions but capable of expanding to complete all the functions of a PFN universally constructed to accept all applications. For these commercial carrier products cost will vary with function and the extent of the system. All the technology is defined within all the related patents. The cost, profit and product pursuits will be determined by market strategy and knowledge of pubic desire for these product offerings.

23D12 is a serial RS232 modem that is capable of handling packet identified or binary Data, Hex decimal data ASCII NEMA protocols and or TTL. This 23D12 modem has the option of being connected to 23D09 a radio frequency either short or long distance but

most generally local unless operated by a licensed amateur radio person using short wave equipment ect bouncing off the ionosphere around the world. These systems

Programmed to digitpeat though an APRS system to connect to an IP Gate way has no limit to sending long distance tracking, either by programmed RF stations or the above Telephony and IP providers however transmission conditions may create reliability constraints in some circumstances.

23D09 short range tracking (Tot Spot) communication can be obtained inexpensively through another modality for the economically compromised (not owning a computer) through the TV and a game style software program caring the calibrated map library the APRS software along with desired zoom functions retrieving the digital data from the 23D12 modem connected to the game control input connector. Of course 23D12 would be connected the same as is done in Figure 23A and the short range RF would be the personal tracking belt would have the same as the protocol and architecture detailed in Figure 23A as well as commercial products consolidated in integrated circuits.

The service providers for the two way Pager systems, and wireless phones would use triangulation locating to the known towers and provide the IP hook up through a intranet to area cable providers as a product to sell to cable sub scribers where they would run a software program for the subscribers to view their children on their own home TV or make a request for specific alerts for when their children were past a certain distance from, e.g., the house. The cable providers world run this in a mass data management computer and the base technology of tracking an asset on the screen is the same as Figure 23A. This would also be a service sold to the satellite companies where they are dominant in the market place.

Up-links and requests are possible for Cable Satellite and Web TV to personalize program service even through TV remotes, and phone land line

COMMERCIAL NOTE: Kline and Walker in the development for the personal tracking and PFN remote monitoring, management and control claims sole proprietor ship for any variation of this product. Which is to track a person pet or a piece of equipment though any wireless pager or telephony systems that is interfaced by IP ISDN ISP or any fiber optics phone rooting system or device, microwave light transmission and provided as a cable, satellite or web TV product to a subscriber to either the TV server or the phone provider or both this also extends to any machine messaging and or monitoring management data as defined In any to any of the related PFN applications. This also extends to any two way component either involving the phone systems or the TV systems either as a combined software interface or as hardware connections.

Kline & Walker will seek out all the same phone systems and pager system as well as

Direct TV and Media General Cable etc. and the Internet providers AOL, Erols etc. for the computer area. This is one way to allow parent of all economic strata to afford inexpensive device to track their children and pets on their own TV as well as receive other Data streams from their child's life experience, when they are not able to be with them or want to be in the back ground. Ultimately the least expensive will be the two way pagers that are tracked through triangulation from the receiving towers and processed by the paging provider and transmitted to the correct TV provider for the pager subscriber for tracking. Still a new technology in the locating system might keep this cost up presently but it will quickly go down with volume. (Of course as detailed this can be done in all the modalities detailed in this application as well as all the related PFN application.

The software will be written to allow a parent to switch to their family channel on their TV and poll their programmed ESN PFN family units and watch their real-time activities. The tracking and object placement of a specific PFN will be accomplished by the same method involving calibrated maps and building architecture as previously detailed. Split screen application will advantage those that have to monitor the disabled, while viewing regular programming.

Or those that need close guarding. And of course gov. tracking of conditionally released people and animals that need to be sent to involved parties can be sent to those individuals directly through their own TVs. (Also monitors can view both parties simultaneously)

Returning to Figure 4 405 is the belt that is completely detailed in Figure 5 23D06 is the Nextel Radio Phone Pager combination or a radio or a cellular phone 407 is a pager basically two way and 23D08 is a GPS receiver if this is used for locating the personal tracking system or PFN.

Figure 23E

This a drawing depicting the many attributes of a personal PFN in the form of a belt, collar harness bracelet, bracket or circular securing device. It is not meant as the only modality or the best modality for carrying out the person or animal PFN set of systems. It is merely employed here to display many of the functions, configurations and uses of this versatile invention. And primarily all personal tracking with accountability and or remote control and management for such an individual device falls within the nature and scope of this invention.

In Figure 23E the belt or collar system is displayed in the closed attached position as viewed from the top as if attached to some one or an animal. And it is also displayed as laid

out in a lower view. The belt has a lot of accessories and it should be kept in mind that in many cases not all accessories would be used however the design of all PFN systems is to universalize a base system in which inexpensive plug and play accessories can be added to the system as desired. The belt systems components will be constructed to allow for varying bracelet/ belt/collar/harness sizes to use the same electronics.

23E00 in the belt itself shown in both configurations top and bottom of the page, 23E01 at the very top is the buckle which will be detailed further as 23E10 and 23E11. 23E02 in the top and bottom vie is a video cam system with audio pickup (Digital or analog - size and cost will determine component) 23E03 shows a top view of a finger thaw for an individual to place their index finger, etc. into upon an identity request either self generated locally by the personal PFN processor on the belt or as a remote communication request from an accountable monitor management and remote control system (Gov. Police agency, hospital or monitoring medical staff. The finger thaw can also be used to determine pulse rate. Of course the sensors are different and if both functions were used simultaneously different transmission circuits would be configured if not hardware wired separate functions would be completed by switching components such as IC's microprocessors and firmware preprogrammed. The main PFN processor will be capable of coupling up to a desk top/laptop desk top and have flash memory burned into EPROM's to run different accessories or accommodate change in functions. Of course if this is a security system crucial code keys timed access and pin numbers as well as any number of security measures will be employed to insure only the authorized personnel make any programming alterations. Programming will also be employed to ready the mechanical lock system in 23E10 to open. This system might require one key with a resistor in it much like the GM vehicles or a card swipe like hotel doors with a magnetic strip or the use of a smart card or chip and reader or a signal sent remotely or inputted though a restricted connection port on the personal PFN system. All of the technology to construct these modalities is detailed in earlier related patent applications as preventive means to restrict the unauthorized use and access to equipment PFNS. So these same or similar modalities can be applied by anyone skilled in the art to construct a secure locking mechanism for the mandated belt application. Of course all these systems would be tamper resistant and capable of detecting and initiating an alert mode that can be configured to alert locally and give prerecorded voice message instructions or alert the remote monitoring addresses and they would be capable of sending preprogrammed messages (either from the remote management system or stored locally) or communicate real-time communication instructions from remote operators either audibly or by text message to an LCD if an accessory or part of a component C.O.T.S. product service for instant message or text

messages.(earphone and collar Mic will be also accessories to help the individual wearing the belt with instructions and directions in a discrete manner—e.g. a useful protocol for the recent parolee and mentally or emotionally challenged. Of course 23E19 will have a panic button to get help from the remote management support system in real-time for the wearer of the belt system.

23E19 is a sensor array which will have a serial RS232 or comparable protocol more probably a USB system connector(at present), nevertheless, all such possibilities are well documented in the prior related PFN applications. It will connect with a unibus cable system running through the belt labeled 23E07. 23E07 will be capable of supporting physical connections in various positions around the belt for accessories and the PFN processor or C.O.T.S. component processor system will be able to drive the components through burned in software programs installed through a computer with the specific commands that are appropriate for an explicit application. The reason that C.O.T.S. processors are mentioned here is because as has been detailed through out the PFN invention for man and machine is the continual consolidation and increased functions of product offerings and the PFN platform is designed to be an accountable organizational interface to perform remote control and management for society. So, it is important to point out that these C.O.T.S. products and integrated circuits of multitasking devices are all with in the nature and scope of the PFN invention.

NOTE :For this reason Kline and Walker LLC will seek out all these named electronic manufactures and service companies in a cooperative effort to marry up and interface in the most economical fashion and commercially beneficial means for all including the end user. (in other words if there is engineered product that can be obtained through a specific modality preferable to a specific manufacture and their engineering staff that full fills the PFN protocol and any standard for such product application Kline and Walker LLC will cooperate, license and work to enhance and complete these products and systems in as amiable manner as possible for all. The major objective being to organize the PFN system and networks to provide accountable activities and management so badly needed for public safety and the environment, while insuring a good fair and just respect for individual's rights and their privacy. These PFN systems are designed to enable and provide more freedom for life's learning experience, while helping to safe guard public and personal safety through real-time remote management and control when needed. Objective PFN Accountability is the management tool for respect for all.

23E19 is representative block of many possible sensors e.g., water sensor, breathalyzer, body temperature, radiation or hazardous material detector, e.g., the Nose, drug

detector, pressure detectors and any measurement transducers that can create a unique electrical signal (Analog, or digital, current sensing, TTL, or digital Binary ASCII Hex decimal or any special data protocol like (NEMA) to provide data to the PFN processor, 513 which is handled by the software and firmware preprogramming for response locally and systemically through reporting these data streams to any remote location. This process is well documented with many modalities throughout all the Prior PFN related patent applications

23E01 the digital camera is also detachable and can be held up to the eye to transmit an image of the iris of the eye to allow for system software presently IBM, Lockheed, or flash 21 digital to confirm identity through secure wireless transmissions timed and reported with GPS location coordinates. This has been discussed in earlier related patent applications for equipment PFNS. With processing and memory continually being reduced in size identity software will be running local as firmware burnt in as application specific software in product protocols to complete on location identity checks as well as needed.

23D04 are contact nodes that can press or conduct through fabric or are provided portholes to make contact with the skin either as sharps or liquid conductent released at the appropriate time to enable a low current of amps and high voltage to disable the wearer of the belt, e.g., a Tazer gun function either by a commercial C.O.T.S. system adapted for this purpose with the trigger mechanism wired to an output function pin of the PFN processor and pulled high or activated to dissipate the short high voltage charge to disable the person or animal. In an other modality this invention would construct this entire system out of a capacitor and relay system with Toshiba driver to operate the relay triggered by the stamp computer or processor (this process already detailed for other applications. The capacitor is energized from the power pack and re energized automatically each time it is fired or dissipated. (Of course if this system is employed the wearer would be informed and medically examined to insure that there is no risk for mortal or fatal damage e.g heart attach or seizure in an activation. This is an extreme measure system and would have strict protocols and rapid response teams accompanying this action.) (The system would be made as impregnable as possible and tamper resistant with alerts accompanying any attempt to deactivate or compromise the system.

23E17 is another extreme Personal PFN control measure. It is an automated medicating device in which a sedating dose of medicine is given remotely or locally by the appropriate authorities with much the same response protocols for it's application. Of course the wearer of the belt would be evaluated for tolerance and effectiveness of the medication used and their general physical condition. On top of 23E13 the PFN processing and memory unit is another connection point indicated by a dark round oval. This connector is also a

multi-pin connector and would support telemetry leads attached to sensors for a heart rate and a blood pressure transducer cuff around the ankle to retrieve blood pressure. These electronic signal would be sent to a remote attending medical staff and recorded in the accountable memory both locally and remotely with audio video location data and time and date markers. The remote management team would monitor the effectiveness of the dose and have a second medication available like adrenelin or steroids to reverse the dose or halt any allergic reaction, while the emergency behavioral response team was in route.

Of course these medications are just an example and medical protocols standards and regulations would have to be set by the appropriate authorities and medical personnel. PACs and automated medication system already exist but this technology has created many remote actuators and anyone skilled in the arts could construct the proper device to complete a successful calibrated injection. The proper dose would be already known and installed in the injection cartridge. If 23E06 alcohol sensor, the breathalyzer or chemical and or drug sensor flagged positive only minute sedative increments would be possible by the program if a violent state was still in progress, while constantly polling heart rate, blood pressure, and respiration through an elastic sensor on the belt. Or possibly 504 shocking system would be used as an alternative or a guided pepper spray canister or compressed tear gas would be activated from the top of the belt buckle. Any and or all would be available to the remote and local behavioral teams to help save or minimize injury to a victim while regaining control and management for a negative situation involving the conditionally released during re-assimilation or managed freedom into or with society.

Note: Of course this is not being recommended for those that are considered a threat to society, e.g., the criminally insane, etc. But those that have marginal social problems substance abuse (intermittent or questionable tendencies toward violence, but are not jailed or found guilty of a crime or are awaiting trial (Bond condition) and can use help, guidance Or those that are going to be released early back into society and or those that know they have a problem and ask for additional help by in watch dog situation.

23E06 leachate alcohol sensor is placed in the small of the back (lumbar) region and sponge covered to allow perspiration to collect and be sampled for pH and aromatic changes that take place during the consumption of some drugs like alcohol. This sensor another transducer will generate a specific signal back to the Personal PFN computer and resident software program for an appropriate preprogrammed and or remote controlled response or for monitoring and management decisions for the conditionally released as an early warning to a possible at risk situation for the individual and or the public. Coupled with real-time,time/date and location data from the GPS 514 through 513 the processor and 512 the

communication system in use on board the remote management and control behavioral response team can be there at the critical time to give protection and serve all parties. 515 is a power pack to be determined with a solar cell for recharging. However, the solar cell would be connected to a area of the body most likely to be exposed to the sun like the shoulders or head. This is discussed in this application and earlier related applications.

518 is to be a event memory storage for applications that require a larger event storage that is provided in the 513 processor area. These memories storage devices could be flash memory, or Sony Memory Sticks™ or any of the memory technologies detailed in all the related PFN patent applications. Also they are protected for accountability comparisons with redundant off board memory storage.

509 just below the unibus 507 that connects all the components physically and supplies power to all the components is a large black line. It can be seen in the top closed view as well depicted as one continuous line. For the mandatory wearing of this belt when the buckle lock is closed and sealed this line is a continuous connection through the buckle and impregnated into the PFN computer compartment which is also enclosed in a tamper resistant package with alert systems(local and remote- a topic well covered-because it is the same application specific protection for all essential components as detailed for all PFNs to be of practical service to be accountable systems) Here 509 caries a special signal generated at one end of the line on a out put pin from the 513 processor and received on an input pin on the other end of the line and the pins reverse their function from input to output by a running program in the processor that also measures the resistance or current levels to detect if anyone has interrupted it or attempted to jumper any connection. Many random signal oscillating firmware programs could be utilized and this is just one modality to insure that the secured belt is not tampered with. Of course any such tampering would set off a flag in the tamper program and all alerts would be activated. 515 power exchange for recharging is accomplished by recharge able batteries at home and an emergency power source enclosed in the protected processor part. This emergency power system will be capable of powering all essentials as determined by application specific protocols. With all the detail in all the related applications anyone in the art can design an appropriate power circuit for the application. Once again 23E10 will be a physical locking system as well as an electrical system and will also use many of the same physical and electronic circuits for locking applications as have been detailed previously. These systems ma be pined and riveted or secured like police manacle locks and chains with harden steel. There is no limit to the best way to achieve a secure system. And all of are within the nature and scope of the invention.

The basic focus of the belt system thus far has been for incarceration or early release

or mentally or emotionally compromised with social disabilities. This belt system or any of the personal PFNS or tracking system have great purposes for just about everyone. It is important to remember that not only are there different modalities to perform tracking and accountable management and remote control for personal PFNs but there are varying degrees of product that can be bought in sections at different times and interfaced through different communication paths for all kind of needs and reasons at different times in a persons life. This is one of the major goals in developing the personal PFN structure with the many manufactures and service providers and to develop a universal plug and play system that can have software burned into it at anytime for different purposes. The Federal Access and Control Technology FACT is well documented as an intricate part to the PFN technology and will not be detailed here, but through the PFN organizational system of accountability PFNs can be configured in anyway for most any purpose, not just used in this belt configuration Additional Sensing harness or apparel to be worn.

Just like the collar or belt system the under harness or wearing apparel will have wiring and sensors that can provide physical telemetry back to a PFN system for processing, recording and reporting to the proper support staff. The system will be able to support automated medicine application systems through secure communication links that require close monitoring while giving real time data as to how the patient is reacting to the prescribed and administered medicinal therapy. Conformation of all orders and telemetry will provide accountability both locally and remotely. These systems can also be used to monitor individuals found to have legal social problems due to substance abuse to help manage and control dangerous human behavioral situations where there is a clear legally acknowledged and confirmed problem recognized by all parties, society and the individual and the use of this system is a condition for increased social freedom with legal and qualified monitoring control and management staff available in real time to all parties at risk. This is not proposed for those found to have uncontrollable violence problems and the use of the system would have to be closely planned regulated and watch dogged by legislators, the justice department and civil liberties. This system could also serve well for the mentally incompetent

From the second PCT patent many personal PFN product offerings are discussed and this section is being quoted here to merely display the early variations and configurations of the PFNs and that the Belt configuration in Figure 23E is merely just one such product offering.

Personal PFNS From Prior Filings

Modular Component Interface Products

Another configuration could take the form and still function as a small carrying case

(like an entire brief case or woman's purse) which would hold a persons desired electronic device array (a mobile office, etc.). This entire case would have a connector (USB) probably on the case or an IR communication port so that it would either jack right into the vehicle secure box or optically communicate with the interface system either where a space was provided for it internally or connected to the connection array bus or (USB) on the front of the secure compartment. And this way the owner could use the interfaced case, charge its components or individual devices and, if so desired, protect it in transit or when s\he was out of his\her car.

There are many manufacturers creating mobile offices out of brief cases that have cell phones, modems, laptops and G.P.S. system for the business man to use on the road, but none that report back location per/se. Ideally these personally carried component systems would be stored and used in the tradition and protection of the invention's secure containment system because of the high cost of the devices. Some existing briefcase products do have chargers but they are not interfaced with the automobile's TTl, analogue or digital logic control system. This is a great benefit to the consumer with this personally owned and operated vehicle diagnostics system and interface. S/he immediately has accountability for any actions taken in the repair of their vehicle and they can have direct contact with any service provider, who can look at the same data give advice and prices or dispute another service providers diagnosis and pricing.

Basically this was taken out of the earlier PCT patent application to show personal PFNs as mobile offices and their ability to interface with the machine messaging PFNs to provide diagnostic functions. The main point being that personal locating devices that report their location to an other location and different forms of personal PFNs that perform accountable remote management and control are all with in the nature and scope of the PFN invention no matter the configuration.

Statement: This details equipment PFNS and also how they can be used with people. All the modalities are using the same belt system to depict the personal tracking and PFN accountable telemetry remote management and control personal product offerings. At the end of the Figure descriptions there will be some product break outs and names for the personal PFN commercial development and focus of this application. However, this is not all the products variations and configurations nor is it all the names the products will be marketed under.

Another application involves Cellular telephone communication. This system can employ the same collars belts and bracelets but they will transmit the location data via the cellular phone system. In some incidences these will be closed systems and in other cases

they will be open to public access. Cost will be defrayed by commercial advertising supporting the network tracking software and providing security software protocols for the general public to use the two way paging system will also employ the same kind of belts and bracelets—and utilize 2way paging to communicate packets of GPS NEMA protocol data to specific Email address where subscribers or commercial advertisers operate a web site with the soft ware to provide secure individual tracking for a commercial operation. While for the most part these systems will utilize some form of GPS NEMA protocol for obtaining tracking data and transmitting it to another remote location, this technology also plans to utilize cellular triangulation for both cellular phones and pager systems to improve indoor tracking by basing the triangulated data from powerful local transceivers with fixed positional grids and running a triangulated algorithm to provide more exact and continuous locating ability.

Note: The TRAC/ FACT program and system mentioned in this last Figure will be in more detail in the formal application and is already incorporated in this application as it is detailed in all the prior PFN applications. TRAC means Trusted Remote Activity Controller and FACT means Federal Access Control Technology. These are the corner stones for providing accountable remote management and control for society and it's institutions both in equipment PFNs and in these Personal PFNs

Figure 24

This Figure is a product list and a check list of suggested modes to carry out any particular product offering.

Keeping this in mind any combination of technologies and modalities covered here and in all the related PFN Applications are possible modalities to construct product offerings as determined by any licensing

Agreements created to commercialize and exploit these PFN patents and product offerings; also the product names here are considered proprietary in every venue and market including any WWW or Internet. Address, or web page or listing or search engine.

NOTE: specific names set aside for the radio repeater or digitpeater technology are as follows-

''TOT SPOT", "HUNT WELL," "PET POINTER", FRIEND FINDER," this is not to say that other PFN technology like pager or wireless telephony may not create products bearing this name, but it will be solely reliant on the discretion of the licensing authority of Kline and Walker LLC.

NOTE: The Paging and Celluar phone technologies have "FAMILY FINDER", "SKI SEARCHER", and "PATIENT PAL", TRAC A CON(EITHER. COM OR. GOV OR

LOCAL POLICE AUTHORITY. Once again these names may use any of the technologies detailed in this application or any of the related patent application, at the discretion of the licensing authority of Kline and Walker LLC . The rest of Figure six is a list of areas to create market product and names from listing Activity controls, sensor systems, and functions.

SHORT DESCRIPTION:

TOT SPOT ----is a tracking device to a send a child's geographic position to a computer screen organizers palm tops (with wired and wireless modems) or a TV using any of the modalities detailed in the PFN technology through out this application and the related filings

HUNT WELL—is a location system that provides map placement on a hand held wireless LCD communicator screen of no shoot trail markers, e.g.,(locations of other hunters wearing or carrying location equipment and supporting a beacon, houses or farms, supporting a trail marker beacon that appear on the screen, before shooting. This system and the complete product construction may use any of the modalities in the PFN technology to provide many different qualities and properties to this product. People can see hunters in area and hunters can see all beacon PFNS or locating transmitting devices (FCC and Tobacco and Fire arms should set special Frequency for this application and PFN beacon transmitters should be supplied to schools, public gathering places etc. roads and known populated areas by the fish and game people in all the states) These systems could uses solar cells and wind generators to provide powered where land lines or batteries will not be a total solution)

PET POINTER – Of course can be used with other animals (application specific attachments to the animal a consideration of course) But is basically a way to track pets on a computer or TV screen or palm top or GPS or Cellular Phone or pager system if they support a display and a map program any are capable of receiving another's device location transmission signal, through any of the modalities detailed in the PFN technology and these devices are all considered to fall with in the nature and scope of the invention (personal PFN and tracking devices)

FRIEND FINDER or FAMILY FINDER or PEOPLE LOCATOR are all Personal tracking devices to track people through any of the technologies many variations detailed for the PFN systems. They may be belt systems, purses, brief cases, concealed in personal valuables that normally accompany the person. These name are being applied to locating system for this purpose. Other names like

LOST AND FINDER or BREAD CRUM BOX or CRIME TRAIL BOX or THEIF CATCHER KIT are reserved for personal possessions that are placed in to a lockable container that will give it's location remotely once stolen either activated automatically or by

the owner or the police. The systems used here can also be any of the PFN modalities to be determined by practicality. It might just as well be a secluded apparatus that is hidden in a valuable or camouflaged. (These systems can be outfitted with accountable recording equipment all part of this technology's PFN systems

TRAC A CON. COM OR GOV this system can use the any of the technologies detailed in the PFN technologies but is a operated in conjunction with law enforcement and has a protocol involving medical expertise, behavior expertise and law enforcement expertise as well as educators and counseling for the public and the parolee or conditionally released. RF systems used for this purpose might well include companies like Lojack and there RF systems.

SKI SEARCHER OR (SKI SEEKER) OR HITCH HIKER OR CAMP TRACKER may also use any of the modalities in these PFN applications and it basically is a way to track skiers on the slopes or cross country and for them to call for help from the ski patrol operators of the ski lodge or the authorities. Can be a limited range and a system operated by the lodge or tracked by the lodge's monitoring system and personally owned transmitting systems (personal tracking and PFNS)using commercial communication providers that are IP linked or phone linked to the ski lodge. Ski patrol location system monitors all incoming sources and places ESN objects on the map as skiers. (software program monitoring all modalities of transmission can be used for other applications as well) converged is accomplished by a multitasking communication operating software program in the monitoring computer at the, e.g., lodge or ski patrol headquarters and using the computers Com Ports for RF and IP phone connections for pager and phone or even monitoring through a TV cable or Satellite provider. (Satellite and Wireless systems will prove more reliable with severe weather considerations)

SWIM SEARCHER OR (SWIM SEEKER) is a tracking system that is water proof – All PFNs are to be in protective containment but this application is of course made water proof, also the power section has a solar cell so that when the swimmer has to float the solar cell can be exposed to the sun to recharge the power source. These systems are made water dynamic or stream line and can use any of the modalities.

PASSENGER POINTER or BOAT BUDDY will be placed in seat cushions life preservers or given to passengers onboard boats, buses, subways, trams, trains and planes to be attached to their person as a beacon to rescuers in the event of a mishap in travel. The system is normally inactive and can be activated automatically or by rescuers or the individual carrier—(protocols to determine best procedures FAA NTSB DOT) (FAA is not going to want transmission in flight. (FAA and FCC will determine frequencies used so as not to compete with black box signal in air travel or accountable PFNs on board)

PATIENT PAL or HEALTH WATCH, this system and accessory arrays track physical location time and date of application specific commands provides an interface platform of monitoring equipment, for remote telemetry and activity controls for medication actuators aggressive remote control, while providing Accountability systems including audio and video, etc. as well as a record of command received prescribed therapy in two locations at least. Also a special automated 911 message can be individually programmed by medical experts or real-time voice communication can take place for the mentally lucid. All the systems are augment incrementally for patient condition and accessories are prescribed as needed.

Figure 25

This drawing is a Figure showing land platforms sea platforms and rail platforms and a basic way to slow stop and secure these pieces of equipment. There is an entire PCT patent application dedicated to vehicle and internal combustion engines and standard breaking systems. Many activity controls are still available and detailed through out the PFN related applications. Basically, this illustration shows a PFN controlling speed and direction for boats, speed and braking for trucks. The guidance systems for trucks is covered in an earlier application, and of course at the bottom rail will have system guidance so also speed and braking are shown here. Additionally, aviation is covered in other related patents as well as land line hookup PFNS and stationary equipment to cover all the equipment PFNS.

CLAIMS

1. A real-time vehicle or equipment management system including a primary focal node (PFN), comprising:

at least one sensory device monitoring and reporting on data including command function results of at least one of peripheral devices and equipment with application specific data and optional application specific geographic coordinates corresponding to the application specific data;

at least one memory, operatively connected to said at least one sensory device, and located in or on the vehicle or the equipment, storing a plurality of interface protocols for interfacing and communicating, said memory equipped with at least one of an application specific backup device and a redundant memory function recording application specific automated and remote control command strings to the peripheral devices that perform automated and remote control functions;

at least one processor responsively connectable to said at least one memory, and implementing the plurality of interface protocols for interfacing and communicating with the plurality of external devices;

a plurality of external devices supported by at least one interface for C.O.T.S. products and accessories, the plurality of external devices interfacing with said at least one processor via at least one of the plurality of interface protocols, including at least one of: pagers, wireless phones, radio frequency equipment, locating equipment systems, cordless phones, laptops, one-way communication device, two-way communication device, and computer organizers, at least one of said plurality of external devices including a report back capability to report the data collected by said at least one sensory device to at least one remote location including the application specific data that is stored in the PFN; and

at least one two-way communication system including at least one security device or routine to condition the signal with at least one security protocol including at least one encryption technology to securely interface between at least one of the plurality of external devices and said at least one processor,

wherein said at least one processor comprises at least a local Primary Focal Node termed a PFN to have hardware and programmable and or modular software or firmware termed TRAC which functions as a Trusted Remote Activity Controller providing robotics or automated and remote control accountability by recording event data local and redundantly in remote memory storage, for communication components and computer hardware systems as determined by any industry or government standards efforts and protocols, for interfacing

with activity controls, sensors, or discretes in any vehicle, machine, or as part of any equipment or on any person, animal, living entity or for any arbitrary use as a free standing piece of accountable telemetry or control equipment.

2. A real-time vehicle or equipment management system including an optional security function that restricts unauthorized access thereto, comprising:

at least one operation sensor recording the operations of the at least one of the vehicle and equipment as a recording signal;

a memory storing the operations of the vehicle or the equipment received from said operation sensor in a secure manner; and

a processor responsively connectable to said memory, receiving the recording signal, at least one communication device reporting or transferring data to at least one remote monitoring and control system with transmission of the data being optionally two-way transmission for memory storage recording of remote control commands, the recording signal from at least one of operation sensor, audio data records and visual data records, said at least one communication device comprising at least one of:

a two-way pager responsively connectable via at least one of a processor and a computer stored in a secured manner and capable of transmitting data to download to at least one remote monitoring system;

a wireless telephone responsively connectable via the at least one processor and computer stored in a secure manner and capable of transmitting data to download to the at least one remote monitoring system;

a radio frequency transceiver responsively connectable to the at least one processor and computer stored in a secure manner and capable of transmitting data to download to the at least one remote monitoring system;

a physical connector interface port responsively connectable to the at least one processor and computer and at least one of protected, shielded and maintained in a secure manner, and capable of transferring data to download to the at least one remote monitoring system;

an optical light data transmission port responsively connectable to the at least one processor and computer and securely maintained, and capable of transmitting data to download to the at least one remote monitoring system;

a multi-tasking law enforcement device capable, optionally through electronic security protocols, to communicate with the at least one processor and computer and download to the at least one remote location;

at least one processor and computer responsively connectable to at least one memory and at least one auxiliary communication device in a secure manner that can be processed to any other communication device responsibly connectable to the processor or computer to download the data to the at least one remote monitoring system;

at least one processor and computer responsively connectable to a Global Positioning System (GPS) able of transmitting GPS coordinate data protocol to the at least one remote monitoring system;

at least one processor and computer responsively connectable to at least one magnetic card swipe device that can transmit via other communication devices to the at least one remote monitoring system for at least one of billing, debiting and crediting;

at least one processor and computer responsively connectable to at least one of audio and video devices and other communication systems to at least one of guide and control remotely a vehicle;

at least one processor and computer responsively connectable to at least one memory to record at least one of an audio and video signal, and data used to control a vehicle remotely; and

at least one two-way communication system including at least one security device or routine to condition the signal with at least one security protocol including at least one encryption technology to securely interface between at least one communication device and the remote location,

wherein said at least one processor comprises at least a local Primary Focal Node termed a PFN to have hardware and programmable and or modular software or firmware termed TRAC which functions as a Trusted Remote Activity Controller providing robotics or automated and remote control accountability by recording event data local and redundantly in remote memory storage, for communication components and computer hardware systems as determined by any industry or government standards efforts and protocols, for interfacing with activity controls, sensors, or discretes in any vehicle, machine, or as part of any equipment or on any person, animal, living entity or for any arbitrary use as a free standing piece of accountable telemetry or control equipment.

3. A real-time vehicle or equipment management system according to claims 1 or 2, wherein said plurality of external devices includes at least one of: an electrical actuating accessory and at least one peripheral device controlling automated remote control functions utilizing at least one of electricity, compressed air, gases, vacuums, hydraulic and fluid pressure.

4. A real-time vehicle or equipment management system according to claims 1 or 2, wherein said plurality of external devices includes at least one of: electro magnets solenoids, motors, mechanical or silicon relays, pistons, cylinders, pumps, valves, adjustable valves pindle valves cables, linkages levers, shifter forks, paws, ratchets, catches, couplers, spring returns, gearing or power transfer mechanisms cases, brake pads disk assemblies, or drums, clutches and/or interlocking drive mechanisms, spined hub collars and shafts.

5. A real-time vehicle or equipment management system according to claims 1 or 2, wherein said at least one of said plurality of external devices include a backup system to provide back up to any automated, remote control system.

6. A real-time vehicle or equipment management system according to claims 1 or 2, wherein said at least one of said plurality of external devices includes at least one of a coyote circuit and other circuit used to create a plug and play connector as a universal modality to interface with at least one of electrical parts, components, devices, C.O.T.S. personal products or different manufactures products.

7. A real-time vehicle or equipment management system according to claims 1 or 2, wherein said at least one of said plurality of external devices includes at least one application used in conjunction with a security system, home computer controller system, household equipment and utilities management system to organize, store, complete phone node contact and transmit data for utility and/or equipment use for any billing, personal records and/or taxing for same, as well as, provide services for repair and maintenance purposes.

8. A real-time vehicle or equipment management system according to claims 1 or 2, wherein said at least one of said plurality of external devices includes the function of operating at a specific location and not being transferrable to another location without authorization, and when transferred in an unauthorized manner, the at least one of said plurality of devices transmits an identification signal to report the location of the displaced equipment.

9. A real-time vehicle or equipment management system according to claims 1 or 2, wherein said at least one of said plurality of external devices are supported by a universal interface for separate C.O.T.S. products and accessories, the at least one of the plurality of external devices interfacing with said at least one processor via the at least one of the plurality of interface protocols, providing the capability of the at least one of the external devices to be at least one of remotely controlled and remotely operated.

10. A real-time vehicle or equipment management system according to claims 1 or 2, wherein said primary focal node supports at least one of application specific software protocols and hardware systems for industry standards for recorded data as determined by at least one of codes, specifications, rules regulations, and laws, for at least one of vehicles, equipment or machinery use.

11. A real-time vehicle or equipment management system according to claims 1 or 2, wherein said real-time vehicle or equipment management system includes redundant remote storage in at least one remote location in at least one application specific industry standard protocol as determined by at least one of codes, specifications, rules, regulations, data handling procedures and laws for at least one of equipment, machinery and vehicle use.

12. A real-time vehicle or equipment management system according to claims 1 or 2, wherein said real-time vehicle or equipment management system is at least one of global network, web and Internet accessible to monitor remote control function in real time and to mass store data off-board as transmitted by the PFN and/or other machine messaging systems and to access the web for personal use from the PFN for E-mail messaging and/or remote tracking either personally, as commercial service and/or for legal and/or governmental reasons.

13. A real-time vehicle or equipment management system according to claims 1 or 2, wherein said real-time vehicle recording system is substantially stored in a stop and control box to prevent unauthorized access thereto and the vehicle.

14. A real-time vehicle or equipment management system according to claims 1 or 2, further comprising a payment mechanism in or on the vehicle, responsively connectable to said at least one processor, said payment mechanism collecting vehicle information and providing real-time billing, debiting or crediting from the vehicle, and retrieving at least one of a script or electronic signature from a card carrier, and verifying the identity of the card carrier via at least one of photograph, fingerprints, and identification.

15. A real-time vehicle or equipment management system according to claims 1 or 2, wherein said at least one processor performs at least one of the following functions:

remotely controlling at least one of robotic functions to activate and control vehicle operations, remotely billing for use of the vehicle, remotely operating at least one machine, evaluating and diagnosing computer or processor malfunctions, remotely ordering materials and service personnel to perform at least one of service and repairs, remotely performing price quotes for cost of the at least one of service and repairs, remotely performing repairs electronically, and remotely shutting down equipment;

remotely controlling data exchange representing a monetary exchange via a focal node to perform a secure and protected containment function of: to restrict unauthorized use of equipment, to record and preserve data in an acceptable legal manner, and to bill at least the vehicle user, thereby providing a total accountability system;

at least one of networking and communicating with at least one gateway to other computers and computer networks that manage data, said gateway determining whether the other computers and computer networks are to be at least one of networked and communicated with to further monitor and store data for at least one of billing, regulatory compliance and legal compliance, and optionally for at least one of social economic and environmental impact;

at least one of networking and communicating with at least one of other computers and computer networks that manage data, including at least one of vehicle location, equipment technical assistance, personal accounting for machine or equipment use, billing, debiting, crediting, vehicle operations, service and repairs; and

monitoring equipment for health and safety conditions potentially adversely affecting the public, including at least one of reckless driving, driver impairment, pollution, vehicle unsafety.

16. A real-time vehicle or equipment management system according to claims 1 or 2, wherein said at least one processor performs at least one of the following functions:

collecting machine message data from said real-time vehicle recording system used to compile data for a public media or web page, and transmitting the machine data thereto;

presenting the machine message data on at least one web page that originated from at least one equipment on said real-time vehicle or from a machine messaging network;

recording and reporting to a monitoring gateway for billing for highway use by the vehicle;

collecting and storing data corresponding to charging at least one electric vehicle;

reporting, recording and billing automatically using a real-time billing system in the vehicle corresponding to time a geographic area roadway is used;

determining impact on environment including roadways, using at least one sensor recording at least one of:

weight and emissions ratings for atmospheric impact type of at least one of fuel and energy used;

time of operational machine use;

amount of fuel or energy used;

type of waste product produced; and

amount of the waste product produced.

17. A real-time vehicle or equipment management system according to claims 1 or 2, wherein said at least one processor performs at least one of the following functions:

recording at least one of audio and video traffic vehicle impact, and recording and reporting to at least one remote monitoring system for at least one accident investigation and machine accidents in a data secure manner;

recording information used in insurance investigations to decide claims and assign liability;

determining liability and accountability to be used in legal proceedings and optionally to be used in determining safety parameters, rules, regulations and laws;

recording at least one of audio and video captured criminal incidents by activating unattended vehicle systems to report criminal events through remote control;

recording at least one of audio and video captured news events as witnessed by a machine system including at least one of weather conditions, and traffic conditions.

18. A real-time vehicle or equipment management system according to claims 1 or 2, further comprising at least one operations sensor recording information including at least one of operations of the vehicle, highway conditions, speed limits, driving conditions including speeding, reckless driving, drunken driving, road rage, pensive or inefficient driving, and wherein the information of the vehicle are received from said operation sensor and stored in said memory and downloaded to at least one of a remote monitoring system, a remote billing system, and a remote data analysis system.

19. A real-time vehicle or equipment management system according to claims 1 or 2, wherein storage of the information includes storage with two onboard and at least one offboard storage of the host piece of equipment, the offboard storage optionally including application specific Email or warning flag detailing an electronic serial number associated with a privately owned or personal E-mail address.

20. A real-time vehicle or equipment management system according to claims 1 or 2, wherein the PFN includes more than one purpose optionally billing for commercial service or for specific service of a machine and simultaneously gathering data on any incident or accident event or provide additional controls by off board control and/or management systems in an emergency or in the case of a compromised operator in real-time.

21. A real-time vehicle or equipment management system according to claims 1 or 2, wherein an electronic serial number (ESN) allows each element within the matrix to be securely and accurately tracked, inventoried or controlled, either through a local control loop or remotely, by an authorized application or agency.

22. A real-time vehicle or equipment management system according to claims 1 or 2, wherein an electronic serial number includes the basis for digital encryption of information passed between the PFN device and the controlling entity with local network processing nodes through public communications channels such as the phone lines or Internet initiated in many cases wirelessly from mobile PFNs accompanied by their Mobile Identification Number.

23. A real-time vehicle or equipment management system according to claims 1 or 2, wherein this programmable software and/or any other accountable software program that performs automated and remote control and/or robotics functions as a result of programming that can authorize, authenticate and preserves commands and save feedback data as a TRAC software program and proprietary to this technology and its nature and scope.

24. A real-time vehicle or equipment management system according to claims 1 or 2, wherein at least one non-volatile memory storage and controlled events are in secured environments so that it is highly tamper resistant through physical means and equally protected through electrical means and tamper resistant software programming to become an agreed upon standard for accountable reliable and trusted software commands and record keeping for passive and aggressive remote control and robotics to analyze, judge, evaluate, value, appraise and monitor, manage and control at least one of vehicle use, machine use, equipment use, facility or installation functions, perform financial transactions in real time and in stationary and mobile settings.

25. A real-time vehicle or equipment management system according to claims 1 or 2, wherein accountable data is provided to an E-mail address web site and/or through the use of the World Wide Web and/or Internet Protocol (IP) for at least one of financial purposes, government uses, service providers, social purposes, environmental purposes.

26. A real-time vehicle or equipment management system according to claims 1 or 2, wherein at least one of modular and programmable routines are determined by the existing hardware and operating system firmware or software for any application responsively connectable through any communication medium by querying each component device attached through a PFN/TRAC system and/or piece of equipment to determine if said connectable component is legitimate and cleared for safe public use.

27. A real-time vehicle or equipment management system according to claims 1 or 2, wherein a registry includes all applicable government agencies with their own access to the Registry and/or network with encrypted codes and Identity command strings which are communicative and also access for the general public and their Private Encrypted Identity codes (PINs, etc.) access to same said registry.

28. A real-time vehicle or equipment management system according to claims 1 or 2, wherein a registry is accessible by a plurality of manufacturers on a worldwide scale with a plurality of security protocols in the marketing of component, devices and equipment and manufacture must provide a program to be given authorization for sale, and wherein the registry will not activate either the component device and/or piece of equipment without authorization, and resale of the component device or piece of equipment will be requested upon each connectable and queried to respond to the nature of the new install as the registry is contacted and requested to activate the unit.

29. A real-time vehicle or equipment management system according to claims 1 or 2, wherein a registry including encryption on the Web will support any and all payment industry software.

31. A real-time vehicle or equipment management system according to claims 1 or 2, wherein record keeping requires at least one of terminal and device electrical serial numbers and personal identification numbers as part of its authorization and authentication program with the time date and any geographic location coordinates or address of all the equipment and systems participating or performing entries or accessing any application folder or event file in storage at any location or part of the registry.

32. A real-time vehicle or equipment management system according to claims 1 or 2, wherein a host piece of equipment will not operate any of its accessories unless it is provided the correct signal from the registry or a security network, and wherein commercial off the shelf (COTS) products utilize the security functions, resulting in immediate and cost effective conversions.

33. A portable primary focal node (PFN) tracking device that is worn by an individual and reports a location to at least one web address through a public server gateway node, or publicly owned provider node using any type of communication system, an additional claim is made for the networking use of any multi-communication capable PFN to relay or repeat shorter range signals for personally worn PFN devices, wherein said PFN includes hardware and programmable and or modular software or firmware termed TRAC which functions as a Trusted Remote Activity Controller providing robotics or automated and remote control accountability by recording event data local and redundantly in remote memory storage, for communication components and computer hardware systems as determined by any industry

or government standards efforts and protocols, for interfacing with activity controls, sensors, or discretes in any vehicle, machine, or as part of any equipment or on any person, animal, living entity or for any arbitrary use as a free standing piece of accountable telemetry or control equipment.

34. A real-time or equipment management system according to claims 1 or 2 that serves as an accountable end user instruction center or audio tutor to deliver E-learning and educational programming via the PFN TRAC System and discretes.

35. A real-time or equipment management system according to claims 1 or 2 that can be converted to the highest government and military security protocols, e.g., DES and DET, for national security public safety, nation briefing functions.

36. A real-time or equipment management system according to claims 1 or 2 that provides write one-time memory storage locally as a secure accountable function to track and identify the source of any tampering or hacking to the PFN/TRAC System.

37. A claim is made for a local Primary Focal Node termed a PFN to have hardware and programmable and or modular software or firmware termed TRAC which functions as a Trusted Remote Activity Controller providing robotics or automated and remote control accountability by recording event data local and redundantly in remote memory storage, for communication components and computer hardware systems as determined by any industry or government standards efforts and protocols, for interfacing with activity controls, sensors, or discretes in any vehicle, machine, or as part of any equipment or on any person, animal, living entity or for any arbitrary use as a free standing piece of accountable telemetry or control equipment.

38. An additional claim is made for a connectable system software termed TRACS to be operational with the PFN/TRAC local devices and capable of receiving PFN routing of the numerous sub programs and the application specific data strings as detailed in all PFN application specifications and creating a secure redundant event memory storage.

39. An additional claim to claim 37 is made for the entire system to provide accurate records of operation and failure as determined by a standards effort to be considered a Trusted system.

40. A further claim is made according to claim 37 for any fail safe or backup system necessary to be qualified as a trusted device and system as determined by any standards effort at any time in the future.

41. A claim is made according to claim 37 that this software and hardware be in a protective encasement application specific to it's environment and purpose and also to be determined by any standards effort at any time in the future.

42. A claim is a made according to claim 37 that the software and hardware have no special encasement provision. and can be constructed in any functional configuration and format.

43. A claim is made according to claim 37 for an electric certified seal mechanism to secure any encased area and to determine if the area has been breached; this device and system is also to be determined by any stands effort or law.

44. A claim is made according to claim 37 for a mechanical locking device or system to secure any encased area.

45. A claim is made according to claim 37 to refer to this modular and programmable software program or any other programming that performs automated accountable remote control and or robotics functions that authorizes, authenticates and preserves commands with feed back data as TRAC software program and proprietary to this technology and this inventions nature and scope.

46. A claim is made according to claim 37, that TRAC software is provided at least a non volatile event memory storage for TRAC event data processed and that it is in secure environments so that it is highly tamper resistant through physical means and equally protected through electrical means and tamper resistant software programming to become an agreed upon in any standards effort for accountable reliable and trusted software commands and record keeping for passive and aggressive remote control and robotics to analyze, judge, evaluate, value, appraise and monitor, manage and control, Vehicle use Machine use, Equipment use, Facility or installation functions, personal use on a person or as a free standing device, to perform; financial transactions in real time and in stationary and mobile settings security checks on components, PFNS and host piece of equipment. Activities

through automated controls and actuators retrieval and processing of data from feed back sensors retrieval and processing data from environmental sensors any arbitrary processing, encoding –decoding encrypting-decrypting, modulation demodulation of any electrical, signals both analog and digital in any language, format or protocol.

47. A claim is made according to claim 37 as proprietary PFN/TRAC software to provide any data to at least one remote location including, any Ethernet or Intranet and or including any wire or wireless IP gateways (PFNS or other) to provide data to E-mail addresses or web sites through the World Wide Web or Internet for financial Transactions or purposes, governmental or public information or safety uses, tracking and telemetry purpose or for any arbitrary service provider use, social purposes, environmental purposes, individual purpose or use and or any undetermined purposes or use.

48. In accordance with claim 37, a further claim is made according to claim two to consider as Proprietary TRAC software protocols with or without this technology's proprietary protected primary focal node or PFN's physical architecture any form of local communication, location equipment and control interface system that reports to a remote location.

49. A further claim is made according to claim 37 for the PFN/TRAC system to be inclusive of any industry standard or certification or endorsement by the insurance industry, government agencies, professional organizations, the general public safety and civil rights groups or commercial interest groups, or industry and commercial research groups or trade organizations regarding legally acceptable data storage or accountable remote control for financial transaction products or for any of the specifications detailed for society and it's institutions to be with in the nature and scope of this invention and be proprietary.

50. A claim is made for TRAC software record keeping to require terminal and or device electrical serial numbers and personal identification numbers as part of it's authorization and authentication program with the time date any geographic location coordinates or address of all the equipment component and systems participating and or performing entries and or accessing any application event to be on file in storage on location or remotely to be proprietary to this invention.

51. A claim is made for an electrical seal system to detect tampering and to provide a water resistant seal protection for any containment for adhering any two surfaces with sophisticated authorization energizing systems.

52. A separate claim is made for a universal communication interface to perform routing functions, repeater and or digitpeating of RF, wire or wireless telephony, paging light communication, sound or voice recognition technology through a processing interface termed a PFN as part of any standard effort or as an independent multi- tasking communication system.

53. According to claim 37 an additional claim is made for a multi frequency scanning transceiver and processor to locate and process any type of wireless communication or wire com link and to process and identify the signals nature and purpose and pass it on in the most efficient pre-programmed manner, to it's final destination and reroute or reconfigure the signal in any available communication format.

54. A claim is made for memory of any data processed through the TRAC system in any PFN to have a local memory and redundant remote memory as determined appropriate for any application specific PFN.

55. A claim is made for any PFN system to provide data, telemetry, or tracking to a private monitoring and control system, a public system or Internet web site, a commercial web page or e-mail site a privately owned TV and or software program system, e.g., video game, a web TV connectable system e.g., cable or satellite with a joint venture with TV servers and Internet protocol Provider.

56. A claim is made for accountable remote control of actuators through the PFN processor.

57. A claim is made for accountability of activity controls confirmed by feedback sensors.

(Amended Sheet)

58. A claim is made for application specific sensing and supplying that data to any form of monitoring or management system through TV computers other PFN devices or other interface arbitrary systems.

59. A claim is made for an Intra net system to serve as an interactive highway using a PFN to process and make accountable remote control and robotics for land vehicles.

60. And additional claim is made in accordance with claim 37 for the use of specialized policing tools laser gun communication other forms of wireless communication device or even employing TOW missile technology to make contact with an illegal and unauthorized vehicle and to perform a stop or slow stop and secure procedure of the vehicle.

61. An additional claim is made according to claim 37 for event memory storage of this event and any application specific event as prescribed by preprogramming or as a result of an authorized remote command.

62. A claim is made for the interfacing or up linking of remote monitor or management systems to create larger intra nets or to interface with the Internet with or without encryption.

63. A claim is made for the PFN/TRAC system to provide communication switching or repeating or digitpeating automatically or through remote or local commands manually or preprogrammed as protocols.

64. A further claim is made according to claim 37 for the local tracking of these communication strings to better locate and make accountable all command data the activities they command and the confirmation of the activity.

65. A claim is made for the PFN/TRAC system to incorporate and interface with all machine messaging networks and computer networks private commercial and governmental in an organized system designed by standards and protocols.

66. A claim is made for a national registry to track and identify all pieces of equipment and components and to authorize their use, tax and or appraise their impact on society's infrastructure and environment.

67. A claim according to claim 37 is made for government agencies national local and world, individuals and commercial interest, and organizations to interact and have special access and Identification.

68. A claim according to claim 37 is made for this national registry system for the tracking of stolen parts components, devices and total products or product systems.

69. A claim is made for the PFN/TRAC system to be provided as any standards effort prescribes this technology to provide a local organizational electrical interface platform to perform accountable remote control and robotics.

70. A further claim is made in accordance with claim 37 for the future up linking of machine messaging networks and computer networks as a PFN/TRAC system determined to make all persons and machinery accountable for their interaction through component FACT identification and recorded communication strings in redundant locations.

71. A further claim is made for the spider eyes program and multitasking law enforcement tool to shut down a vehicle through real-time discrimination and identification of equipment and all individuals involved in any event and to provide account ability in all locations in real time, locally in subject vehicle as well as in the police cruiser or memory storage device, and at any local police dispatch, and also in state police monitoring system and nationally at the FBI or justice dept.

72. A further claim according to claim 37 is made for the PFN/TRAC system to provide the means to administer and create a track able record of any such shut down no mater what the means used to deactivate a subject vehicle being operated in an unauthorized or unsafe manner as determined by law, any standards effort, and involving any civil liberties or civil watch dog group.

73. A claim is made for automated and remote-controlled communication routing of wireless or land line to and including fiber optic technology through transmission connectables, switches, computer processors, and TRAC programming in the Primary Focal Node, as part of a repeating function for radio frequency digitpeating, wireless telephony, wire and fiberoptics to increase both land line, and wireless service inexpensively through existing or reduced land line wireless and fiber optic hardware.

74. A claim is made for TRAC/FACT programming and hardware system to interconnect all communication intranets for government, military, rail, sea, aviation, commercial, agricultural, law enforcement, EPA, etc., including commercial servers and providers through the TRAC/FACT protocol.

74. A claim is made for the PFN/TRAC System and functions in accordance with claims 1, 2, 33, 37, 38, 50, 51, 52, 54, 55, 56, 57, 58, 59, 62, 63, 65, 66, 69, 71, 73 or 74 to be consolidated and integrated on a chip, as sets of Systems On a Chip (SOC).

75. A claim according to claims 33 or 51 or 52 is made where in, any standard that dedicates any frequencies for communication for remote control or wireless machine messaging, for mobile applications, portable or personal communicating devices, that employ any scanning, process and or rerouting, repeating digipeating, transcribing through high applications and re-transmitting, on other frequency process, and optionally maintains a traceable record.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 December 2000 (21.12.2000)

PCT

(10) International Publication Number
WO 00/78057 A1

(51) International Patent Classification⁷: H04Q 1/00, H04B 7/185, H04M 11/00, G01S 5/02, G06F 7/04, 13/00

(21) International Application Number: PCT/US00/16381

(22) International Filing Date: 15 June 2000 (15.06.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/139,759	15 June 1999 (15.06.1999)	US
60/176,818	19 January 2000 (19.01.2000)	US
60/	1 May 2000 (01.05.2000)	US

(71) Applicant *(for all designated States except US)*: KLINE & WALKER, LLC [US/US]; 11201 Spur Wheel Lane, Potomac, MD 20854 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: WALKER, Richard, C. [US/US]; 15000 Hunters Harbor Lane, Waldorf, MD 20601 (US).

(74) Agents: DONNER, Irah, H. et al.; Hale and Dorr LLP, Suite 1000, 1455 Pennsylvania Avenue, Washington, DC 20004 (US).

(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

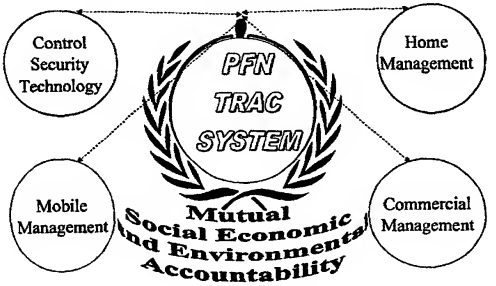
— *With international search report.*

— *With amended claims.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SECURE, ACCOUNTABLE, MODULAR AND PROGRAMMABLE SOFTWARE TRAC

PFN/TRAC REMOTE MANAGEMENT SYSTEMS



(57) Abstract: An accountable modular and programmable software termed TRAC (fig. 1) used generally in a Primary Focal Node (PFN) that authorizes and authenticates commands received from wireless and land line telephone and paging or RF systems or light transmission technologies to remotely activate and confirmed automated controls and functions through processors or controllers and/or computers (402) and create accountable records locally and/or remotely (fig. 4). TRAC processes this data in a secure manner. TRAC stores in a protected storage (406) on board a piece of equipment and reports back to local or the remote location.

WO 00/78057 A1

Fig.A1

PFN/TRAC REMOTE MANAGEMENT SYSTEMS

wo 00/78057
1/64
10/018095
PCT/US00/16381

FIG 1

TRAC

Trusted Remote Activity Controller

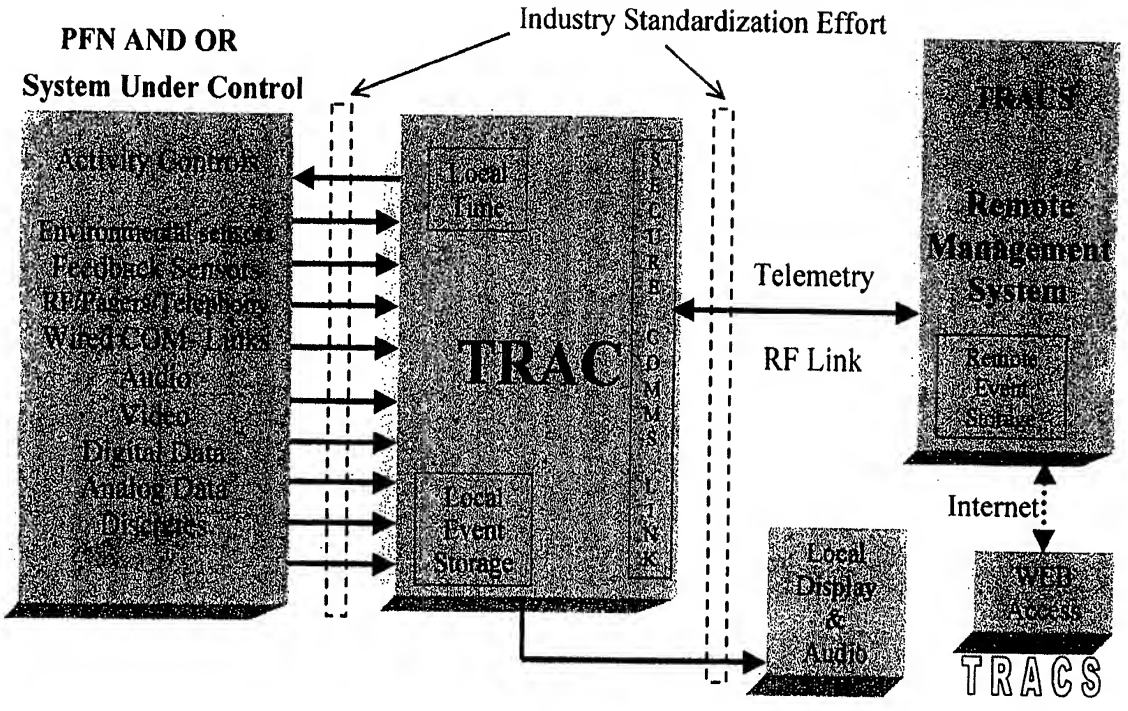


FIG 2

Trusted Remote Activity Controller

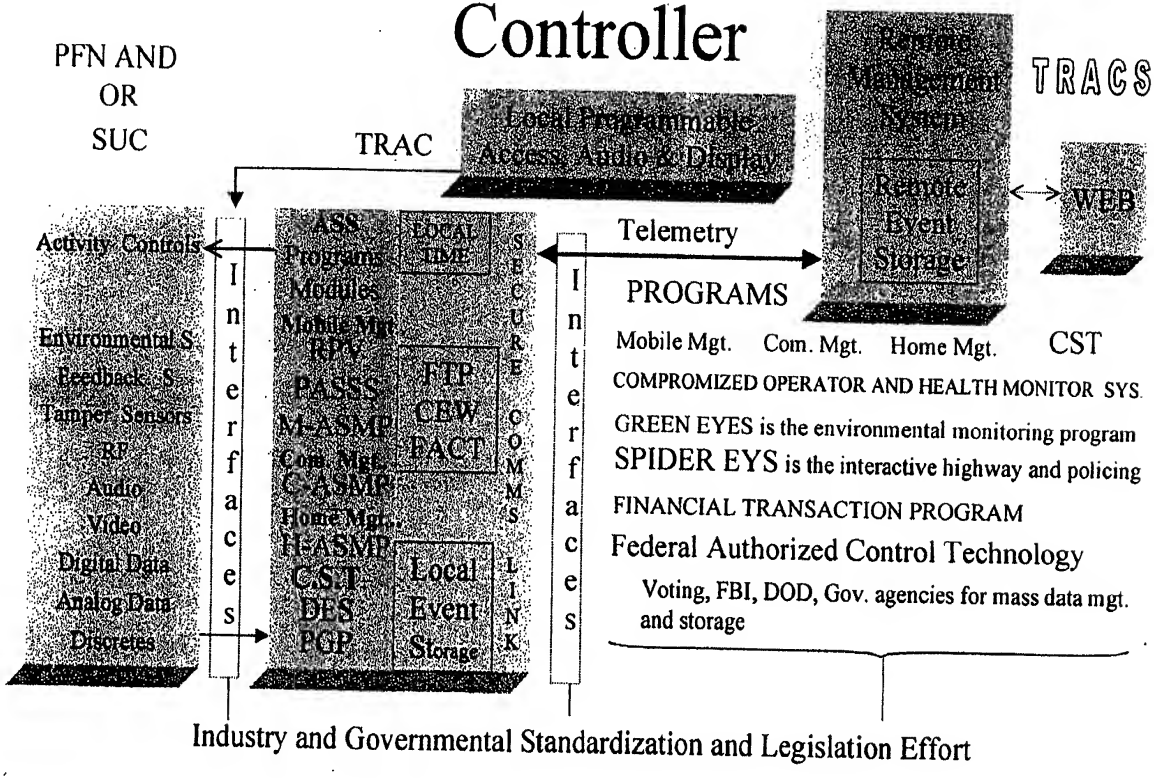
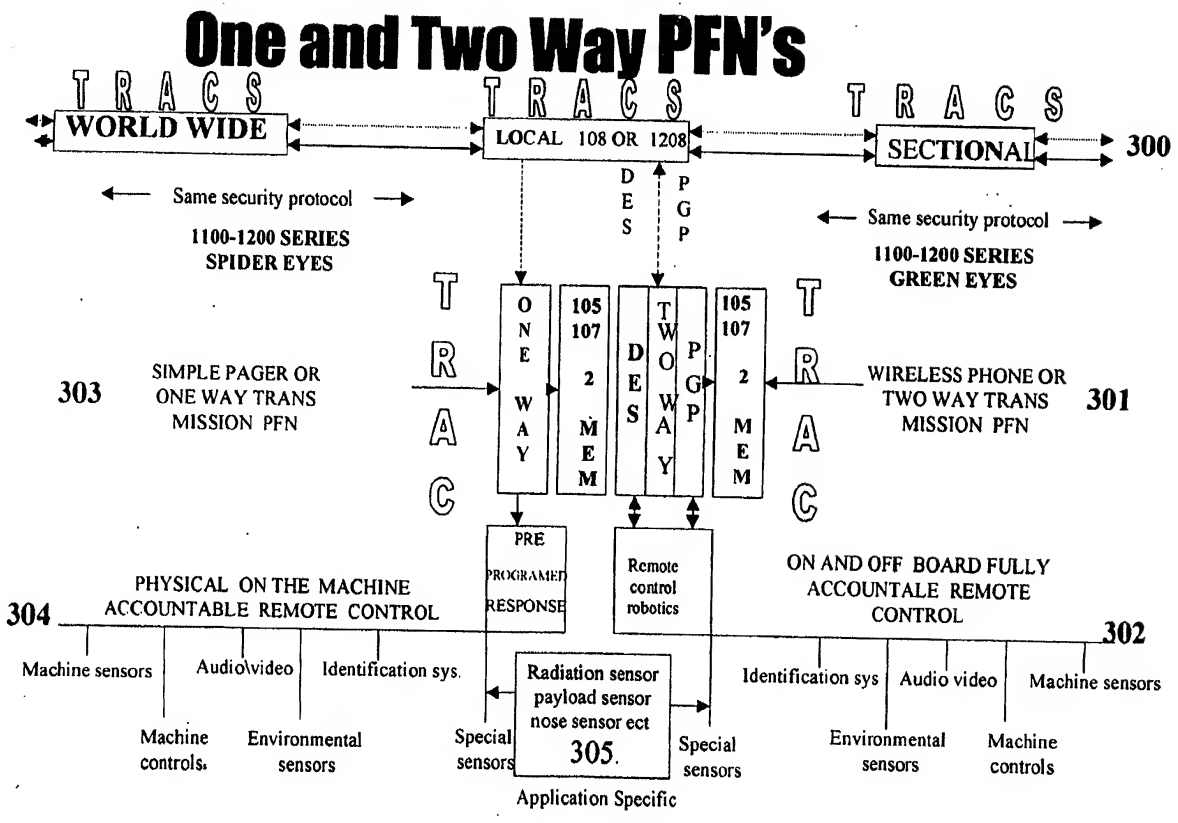


FIG 3



wo 00/78057
4/64
PCT/US00/16381

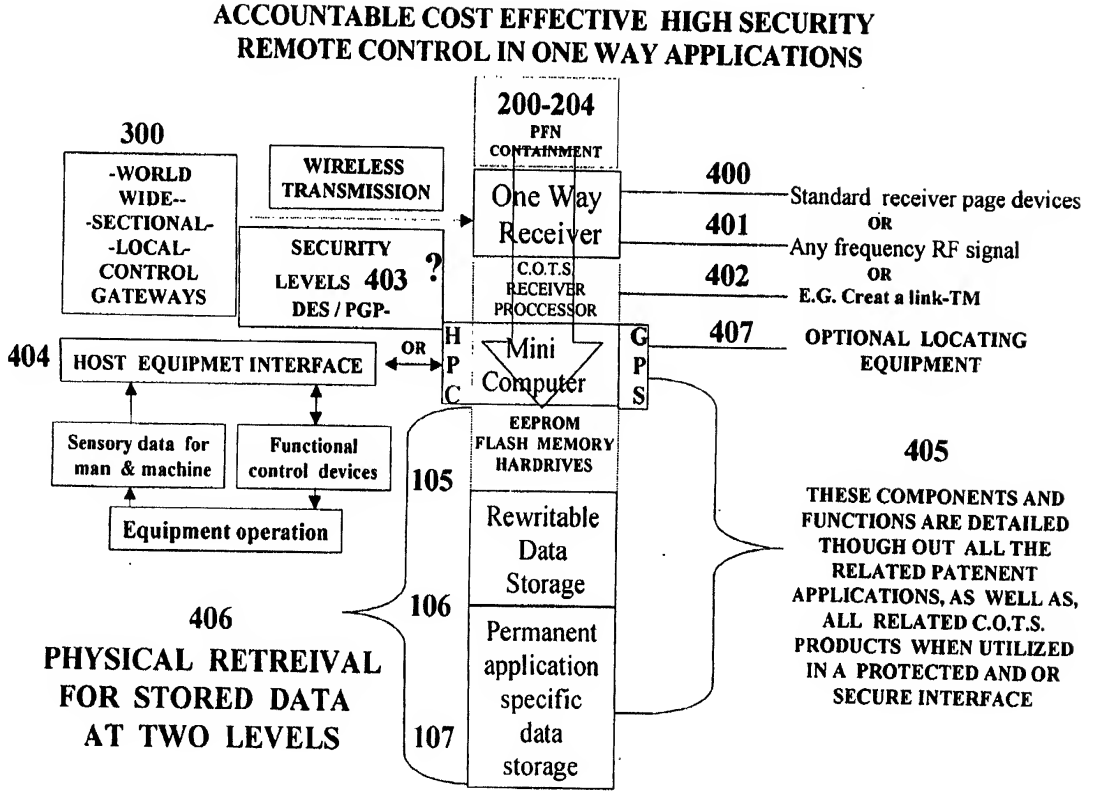
FIG 3A PFN DATA STORAGE PROPERTIES

COMMMUNICATION	AUDIO VIDEO	MACHINE CONTROL AND TELEMETRY	PERSONEL TELEMETRY	ENV. TELEMETRY
1 WAY PAGE	R-O	R-O	R-O	R-O
1 WAY RF SIGNAL	R-O	R-O	R-O	R-O
2 WAY PAGE	R-O-r-RR mc	R-O-r-RR-mc	R-O-r-RR-mc	R-O-r-RR-m
PHONE	R-O-r-RR	R-O-r-RR	R-O-r-RR	R-O-r-RR
2 WAY RF SIGNAL	R-O-r-RR	R-O-r-RR	R-O-r-RR	R-O-r-RR
CORDLESS PHONES	R-O-r-RR-LD	R-O-r-RR-LD	R-O-r-RR-LD	R-O-r-RR-LD
SHORT RANGE RF SIG.	R-O-r-RR-LD	R-O-r-RR-LD	R-O-r-	
RR-LD				

RECORD = R REPORT= r ONBOARD= O REMOTE RECORD =RR
MINIMUM CAPACITY=mc
LIMITED DISTANCE =LD

wo 00/78057
5/64
PCT/US00/16381

FIG 4



wo 00/78057
6/64
PCT/US00/16381

FIG 5

ACCOUNTABLE COST EFFECTIVE SECURE PFN REMOTE CONTROL IN TWO WAY APPLICATIONS

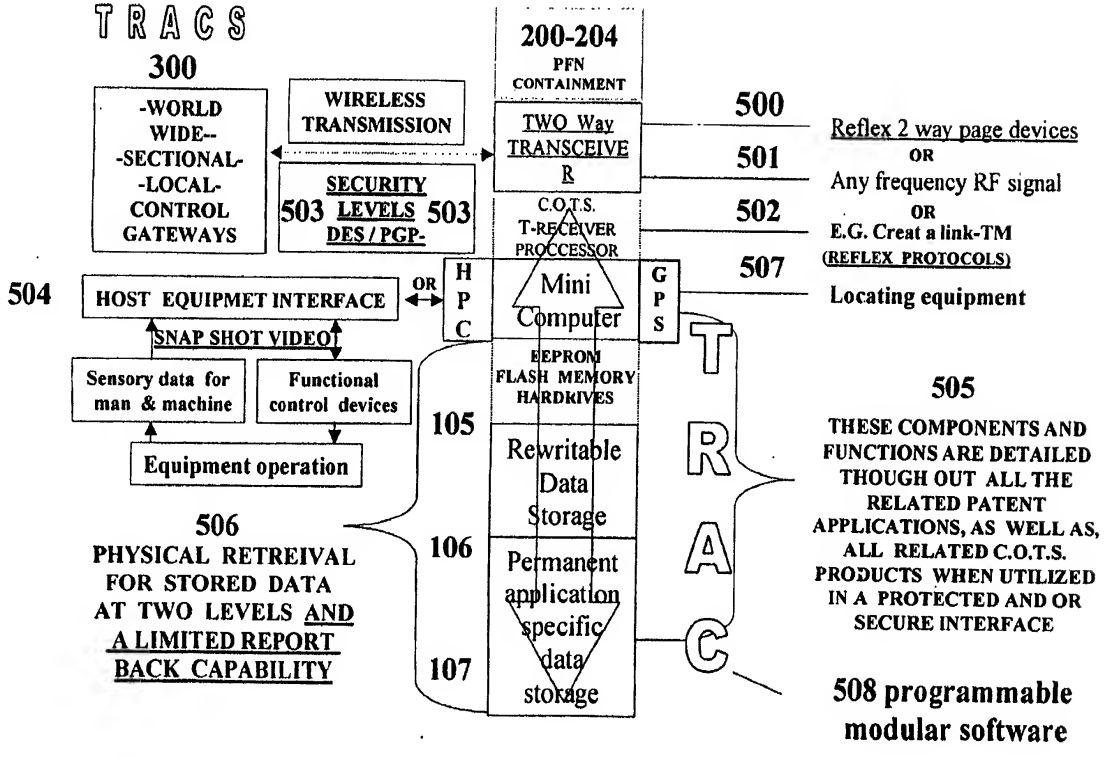


FIG 6

SOPHISTICATED SECURE PFN REMOTE CONTROL WITH TWO WAY APPLICATIONS

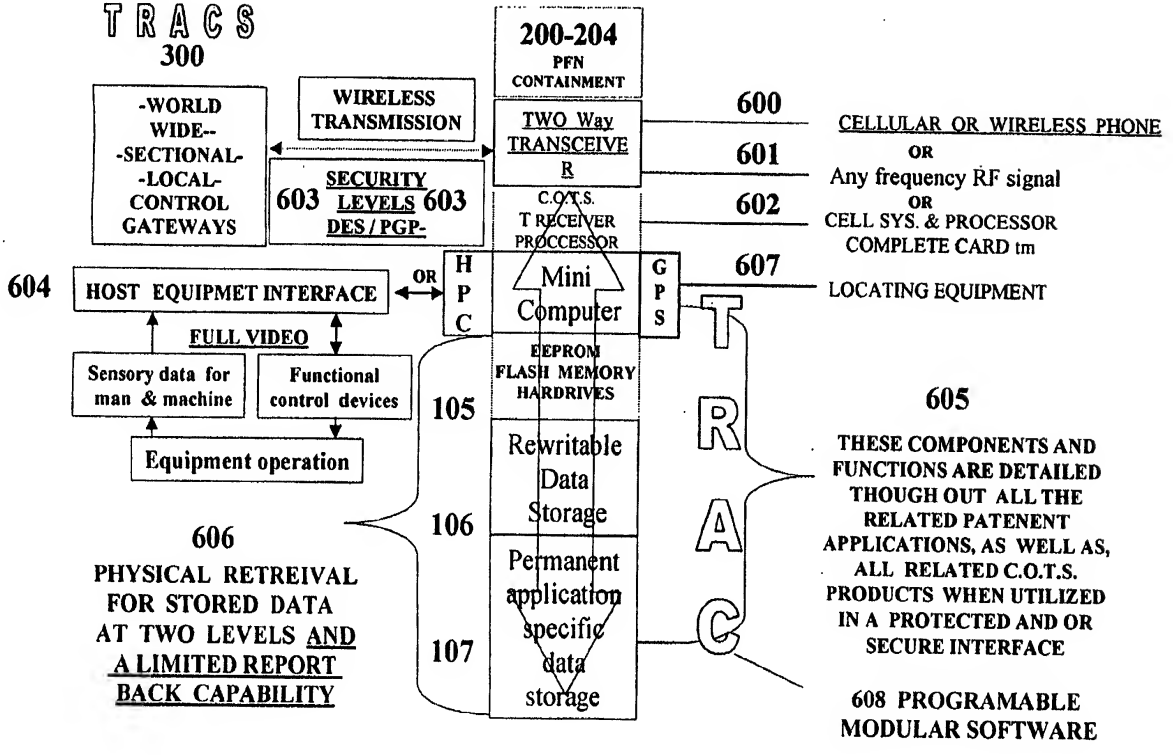


Fig 6 a

PRESENT TO FUTURE PROTECTED PRIMARY FOCAL NODE CONSOLIDATIONS

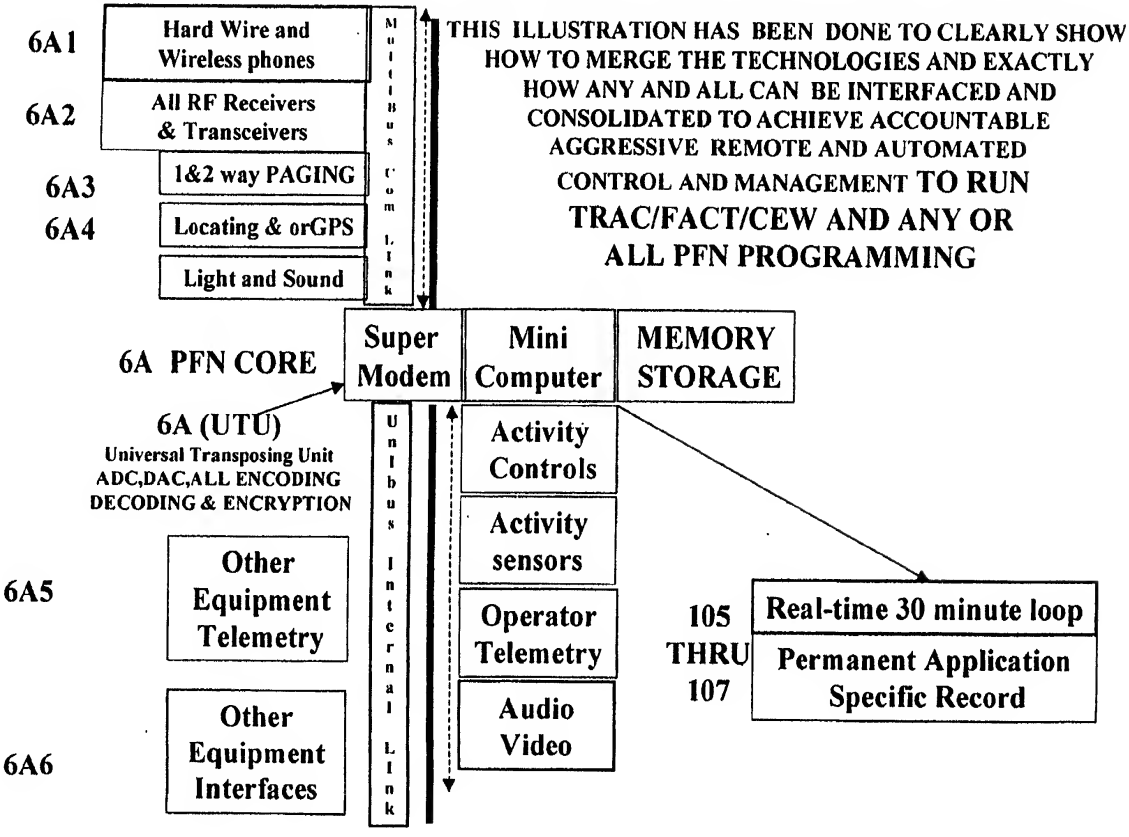
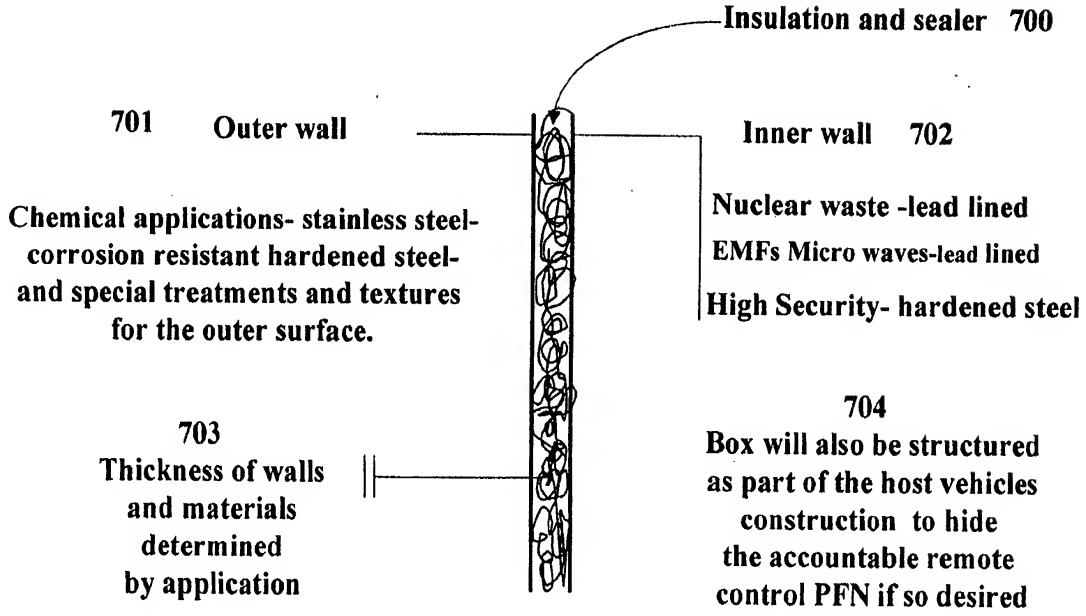


FIG 7

Application specific wall structures for PFNs

NOTE: THESE COMPONENTS ARE FOR EXTREME ENVIRONMENTAL USE REGULAR VEHICLE APPLICATION WOULD HAVE THE PROTECTION OF THE VEHICLE AND CABIN AND WOULD BE SCALED BACK ACCORDINGLY



wo 00/78057
10/64
PCT/US00/16381

FIG 7A

Application specific wall structures for PFNs

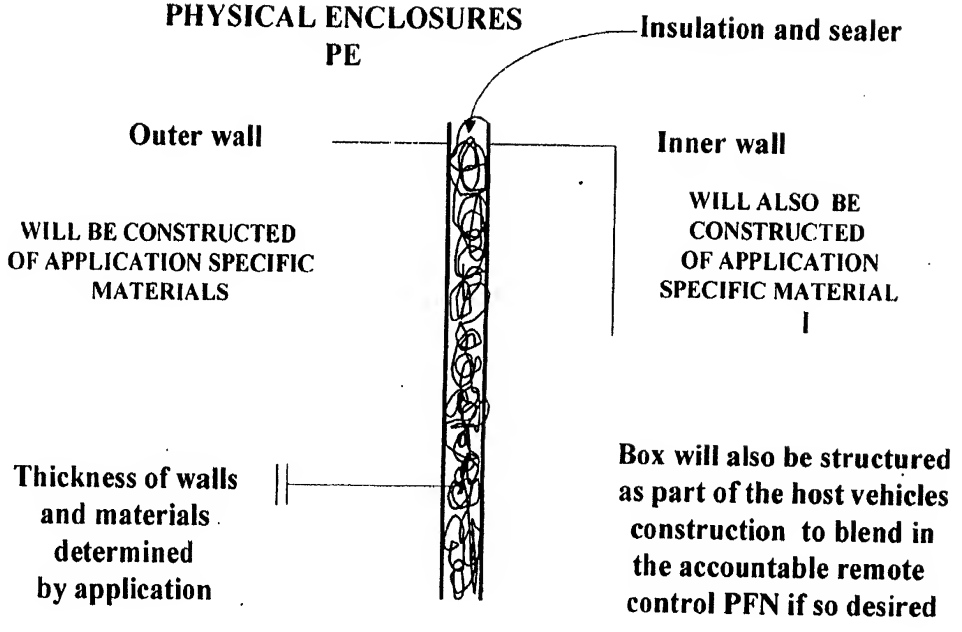
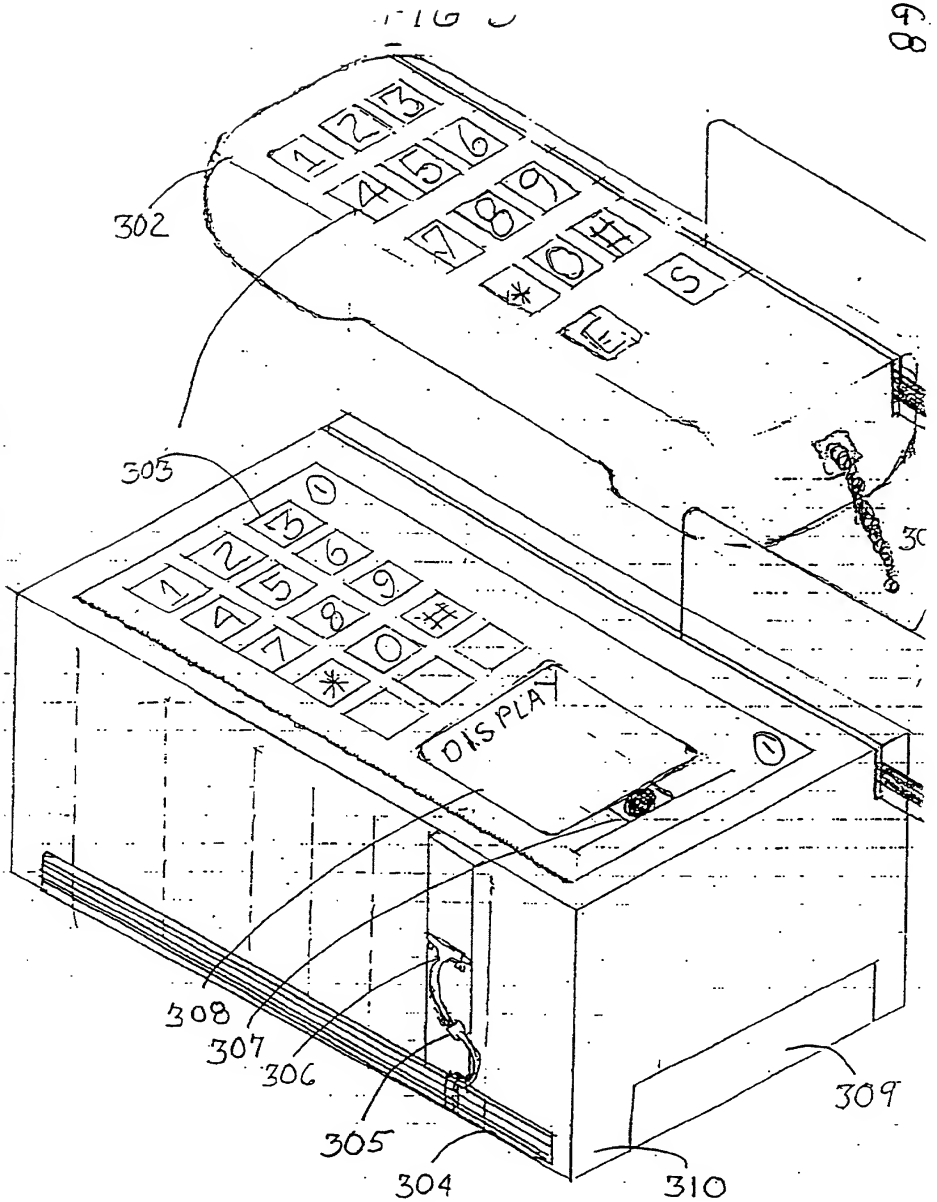


FIG 8



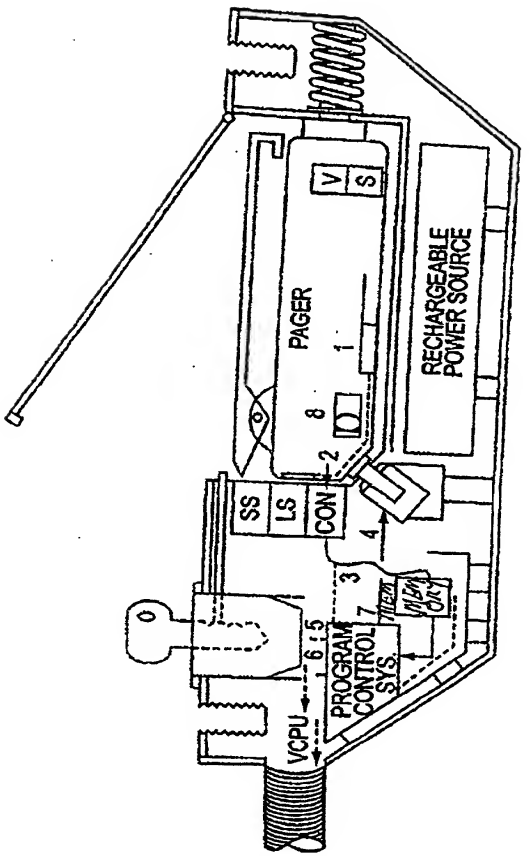
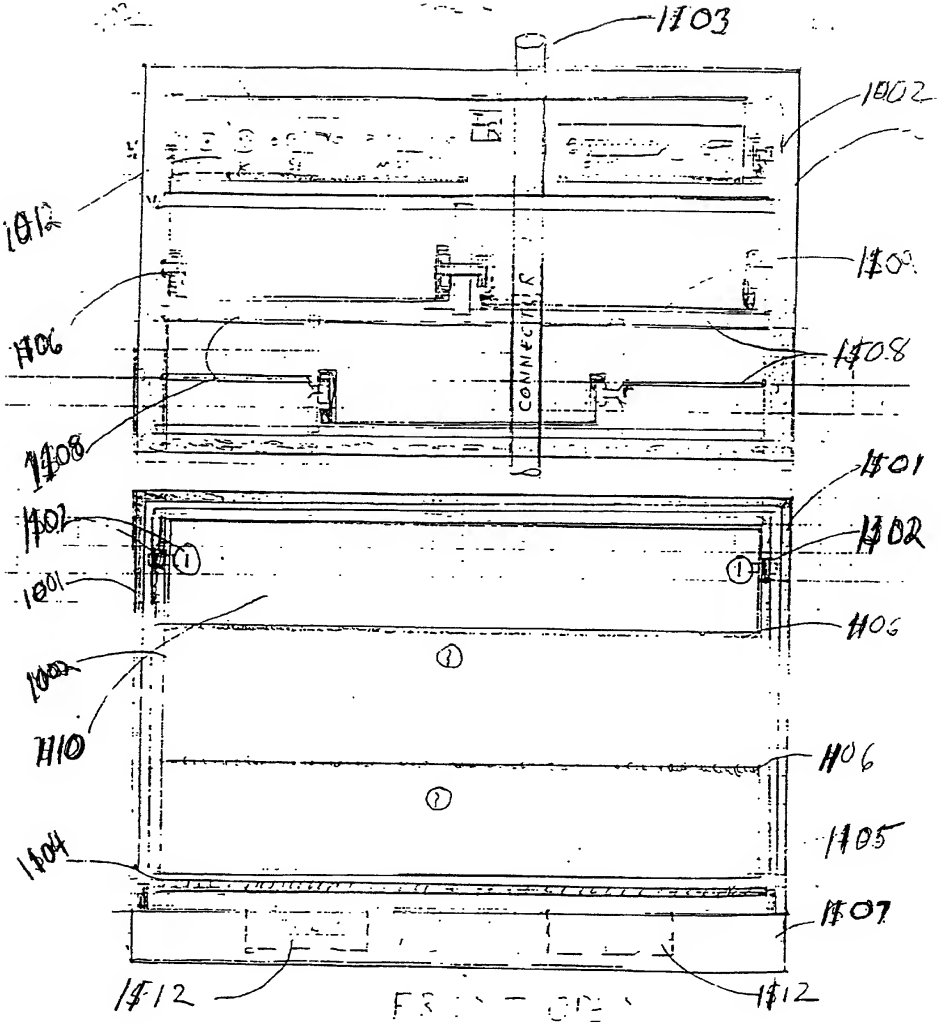

PAGER
V
S
ID
RECHARGEABLE POWER SOURCE
SS
LS
CON
VCPU
PROGRAM CONTROL SYS.
1
2
3
4
5
6
7
8

FIG. 9

Fig 10

Figure 11



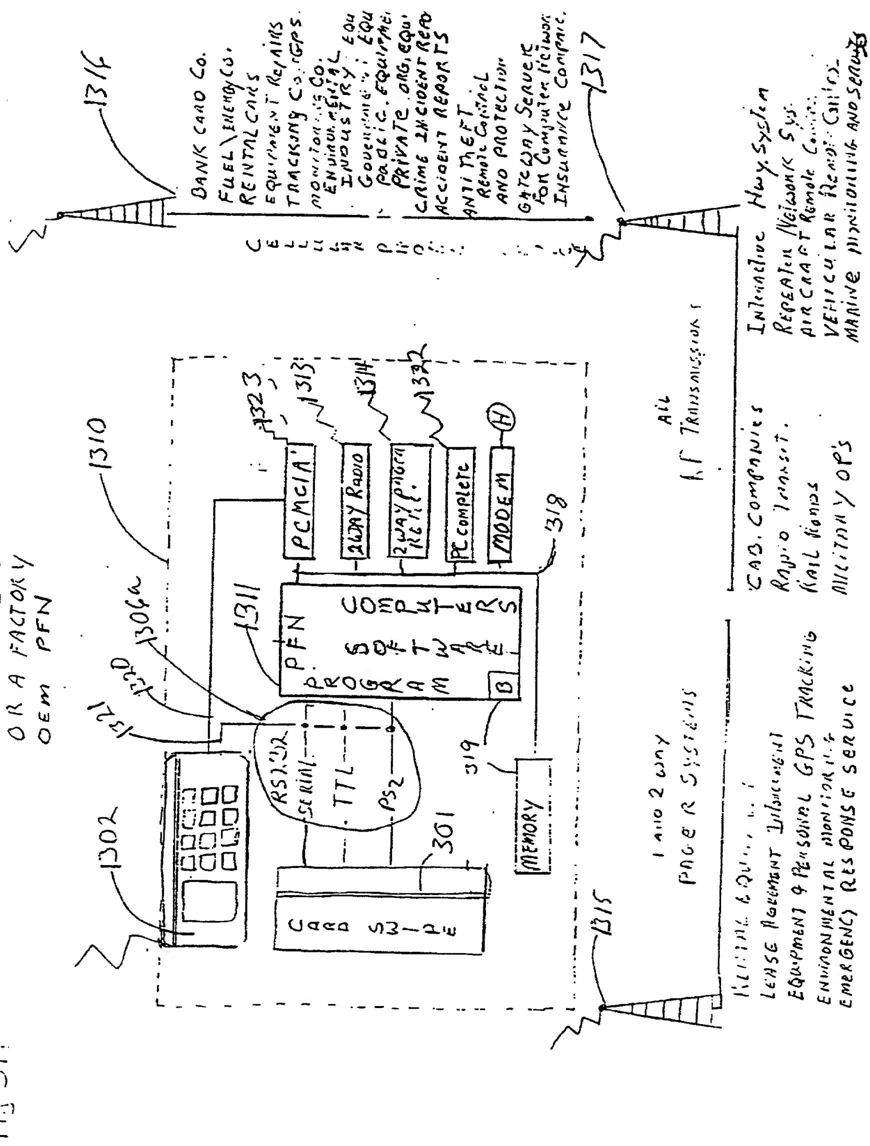
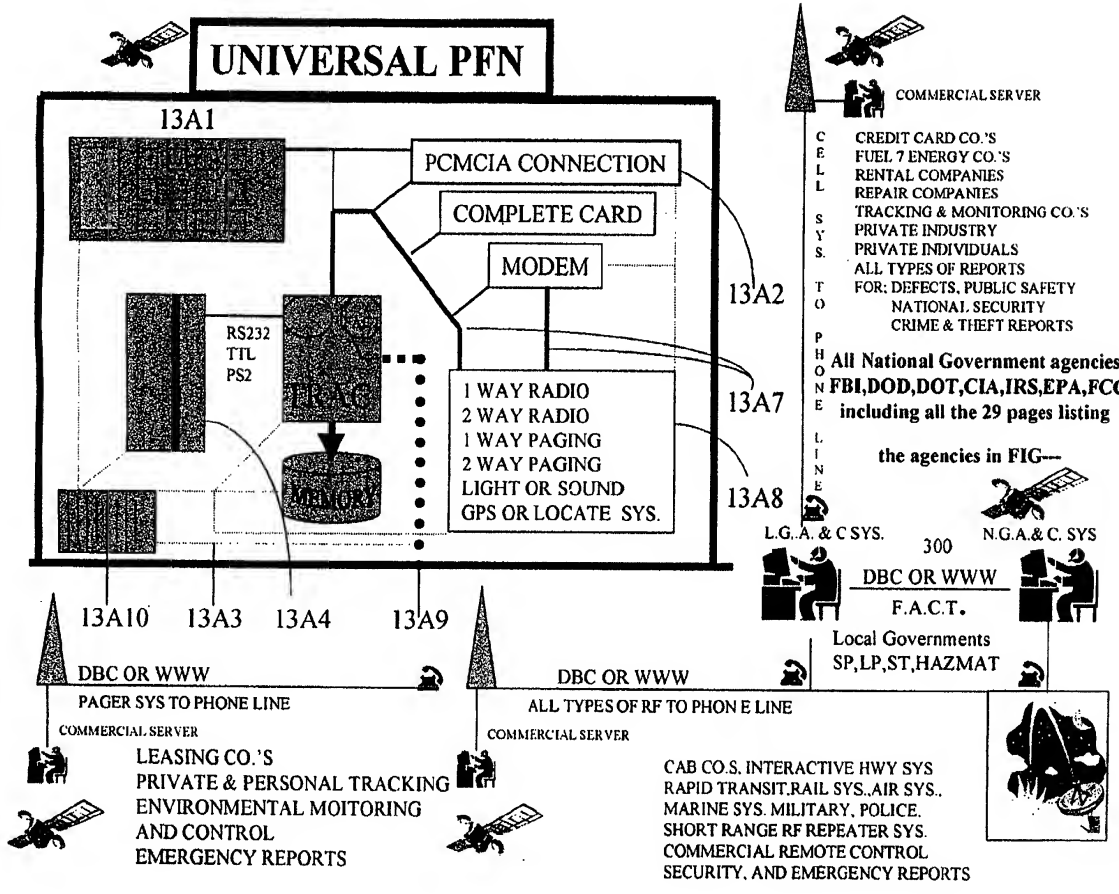

1316
BANK CARD Co.
FUEL\ENERGY Co.
RENTAL CARS
EQUIPMENT REPAIRS
TRACKING Co. GPS.
INDUSTRY
PRIVATE ORG, EQUI
CRIME INCIDENT REPO
ACCIDENT REPORTS
ANTI THEFT
AND PROTECTION
GATEWAY SERVER
INSURANCE COMPANIES
1317
Interactive Hwy System
REPEATER/NETWORK SYS.
AIRCRAFT Remote Control
VEHICULAR Remote Control
MARINE MONITORING AND SERVICES
1310
1323
1313
1314
1322
PCMCIA
2WAY RADIO
PC COMPLETE
MODEM
318
1311
PFN
PROGRAM
COMPUTERS
SOFTWARE
B
1306a
1320
1321
RS232
SERIAL
TTL
PS2
319
MEMORY
1302
301
CARD SWIPE
1315
RF Transmissions
CAB. COMPANIES
RAPID TRANSIT
RAIL ROADS
MILITARY OP'S
1 AND 2 WAY
PAGER SYSTEMS
LEASE AGREEMENT
EQUIPMENT & PERSONAL GPS TRACKING
ENVIRONMENTAL MONITORING
EMERGENCY RESPONSE SERVICE
OR A FACTORY
OEM PFN

FIG 13

FIG 13a



Electronic Security Seal

FIG. 14

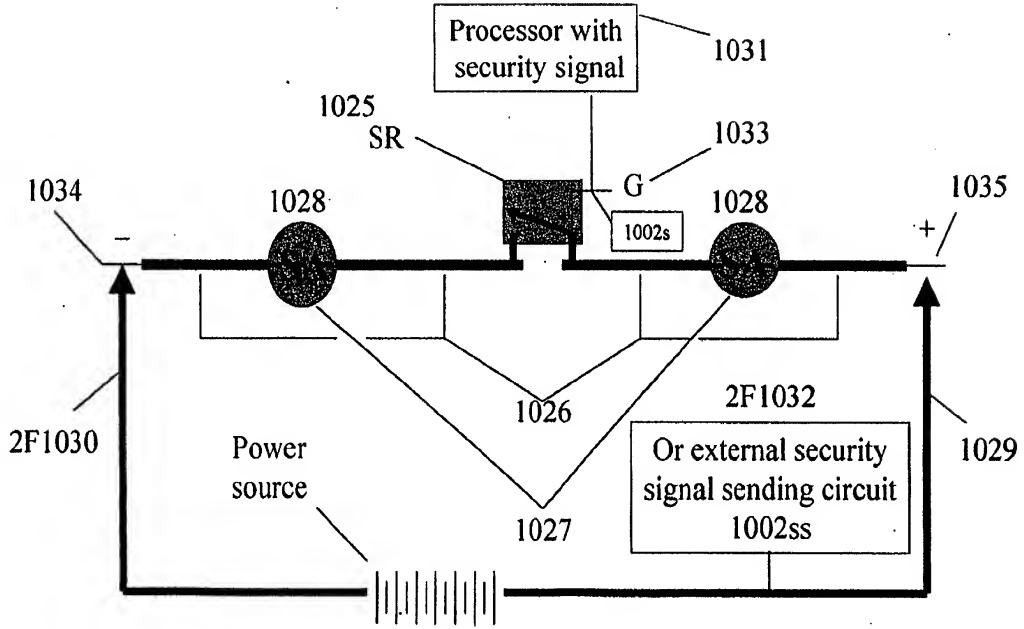
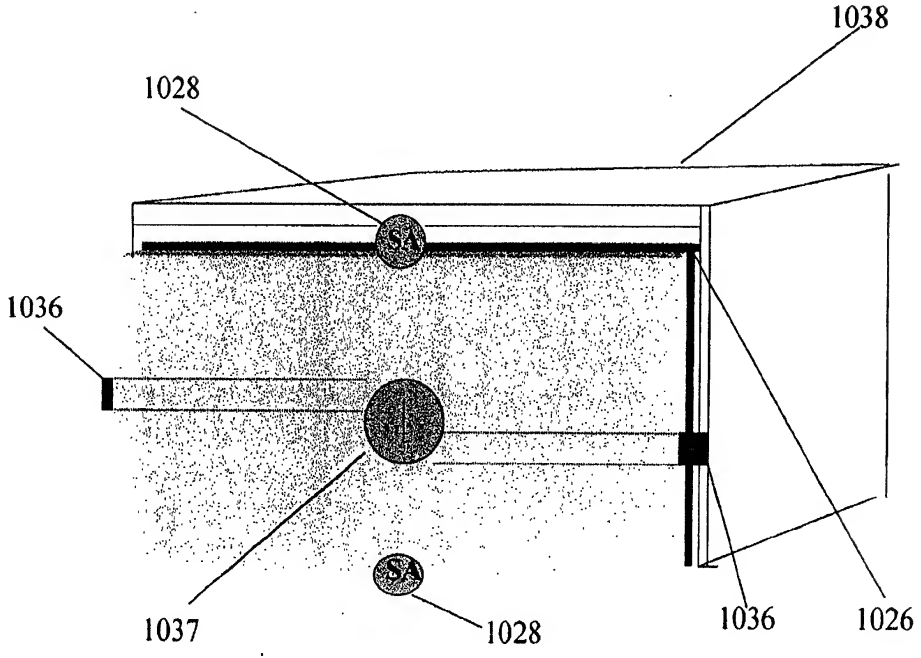


FIG.15

Security Sealed Area For The PFN



U.S. Federal Government Agencies Fig 2A

FIG 16

LSU Libraries

U.S. Federal Government Agencies Directory

A List of Federal Agencies on the Internet

Read a scope note and see yesterday's access stats
View the awards, honors, and recommendations we have received.
Last updated Friday, 06-Nov-98 08:49:24 Send updates and corrections to *Smittie Bolner* (sbolner@lsu.edu).

Keyword search of Federal Agencies
(or use your browser's **Find** command)

Executive | Judicial | Legislative | Independent | Boards, Commissions, and Committees | Quasi-Official

Executive Branch

Executive Office of the President
- White House Office
- Office of the Vice President of the United States
- Office of the First Lady
- Council of Economic Advisers
- Council on Environmental Quality
- National Economic Council
- National Security Council
- Office of Administration
- Office of Management and Budget
- Office of National Drug Control Policy
- Office of Science and Technology Policy
- President's Council on Sustainable Development
- President's Foreign Intelligence Advisory Board
- United States Trade Representative
- White House Office for Women's Initiatives and Outreach

Executive Agencies

Department of Agriculture
- Farm and Foreign Agriculture Services
  - Farm Service Agency
  - Foreign Agricultural Service
  - Commodity Credit Corporation
  - Risk Management
- Food, Nutrition, and Consumer Services
  - Food and Nutrition Service

U.S. Federal Government Agencies

- Food Safety
  - Food Safety and Inspection Service
- Marketing and Regulatory Services
  - Agricultural Marketing Service
  - Animal and Plant Health Inspection Service
  - Grain Inspection, Packers and Stockyards Administration
- Natural Resources and Environment
  - Forest Service
  - Natural Resources Conservation Service
- Research, Education and Economics
  - Agricultural Research Service (ARS)
    - National Agricultural Library
      - Agricultural Genome Information System
    - Pasture Systems and Watershed Management Research Lab (PSWMRL)
    - Subtropical Agricultural Research Laboratory
    - Water Management Research Laboratory (WMRL)
  - Cooperative State Research, Education, and Extension Service
  - Economic Research Service
  - National Agricultural Statistics Service
- Rural Development
  - National Rural Development Partnership (NRDP)
  - Rural Business-Cooperative Service
  - Rural Housing Service
  - Rural Utilities Service
- Office of the Chief Economist
  - Agricultural Labor Affairs Coordinator
  - Office of Risk Assessment and Cost-Benefit Analysis (ORACBA)
  - World Agricultural Outlook Board
- Alternative Agricultural Research and Commercialization Center (AARC)

- Department of Commerce
  - Office of the Secretary
    - Staff Offices
      - Office of Consumer Affairs
      - Office of Business Liason
      - Office of General Counsel
      - Office of Public Affairs
    - Administrative Offices
      - Herbert C. Hoover Building Library
      - Human Resources Management
      - Office of Small and Disadvantaged Business Utilization
  - Office of the Inspector General
  - Bureau of Export Administration
  - Economics and Statistics Administration
    - Bureau of Economic Analysis (BEA)
    - Bureau of the Census
      - CenStats

U.S. Federal Government Agencies

- STAT-USA (formerly Office of Business Analysis)
- Economic Development Administration
- International Trade Administration
  - U.S. and Foreign Commercial Service
    - Export Assistance Centers
  - Import Administration (IA)
  - Market Access Compliance (MAC)
    - Trade Compliance Center
  - Trade Information Center
- Minority Business Development Agency
- National Oceanic and Atmospheric Administration (NOAA)
  - Coastal Ocean Program (COP)
  - High Performance Computing and Communications (HPCC)
  - National Environmental Satellite, Data, and Information Service (NESDIS)
    - Environmental Information Services (EIS)
    - National Climatic Data Center (NCDC)
    - National Geophysical Data Center (NGDC)
    - National Oceanographicic Data Center (NODC)
    - Office of Satellite Data Processing and Distribution
  - National Marine Fisheries Service (NMFS)
  - National Ocean Service (NOS)
  - National Weather Service (NWS)
  - Office of Global Programs
  - Office of Oceanic and Atmospheric Research
    - Environmental Research Laboratories
      - Aeronomy Laboratory
      - Atlantic Oceonographic and Meteorological Laboratory
      - Air Resources Laboratory
      - Climate Diagnostics Center
      - Climate Monitoring and Diagnostics Laboratory
      - Environmental Technology Laboratory
      - Forecast Systems Laboratory
      - Geophysical Fluid Dynamics Laboratory
      - Great Lakes Environmental Research Laboratory
      - National Severe Storms Laboratory
      - Pacific Marine Environmental Laboratory
      - Space Environment Center
  - Office of Research and Technology Applications (ORTA)
- National Telecommunications and Information Administration
  - Institute for Telecommunications Sciences
- Patent and Trademark Office
  - U.S. Patents Database at CNIDR
- Technology Administration
  - National Institute of Standards and Technology
  - National Technical Information Service (NTIS)
    - FedWorld Information Network
  - Office of Technology Policy

U.S. Federal Government Agencies

- Department of Defense (DefenseLINK)
  - Office of the Secretary of Defense
    - Office of the Executive Secretariat
    - Office of General Counsel
    - Office of Inspector General
    - Under Secretaries of Defense
      - Office of the Under Secretary of Defense for Acquisition and Technology (ACQWeb)
      - Office of the Under Secretary of Defense (Comptroller)
        - Department of Defense National Performance Review Activities
      - Office of the Under Secretary of Defense for Personnel and Readiness
      - Office of the Under Secretary of Defense for Policy
  - Joint Chiefs of Staff (JCSLink)
    - Joint Staff
      - Directorate for Manpower and Personnel (J-1)
      - Directorate for Intelligence (J-2)
      - Directorate for Operations
      - Logistics Directorate (J-4)
      - Strategic Plans and Policy Directorate (J-5)
      - Directorate for Command, Control, Communications, and Computer System (J-6)
      - Operational Plans and Interoperability Directorate (j-7)
      - Force Structure, Resources and Assessment Directorate (J-8)
      - Directorate of Management
    - Defense Agencies
      - Advanced Information Technology Services--Joint Program Office (AITS-JPO)
      - Armed Forces Radiobiology Research Institute (AFRRI)
      - Ballistic Missile Defense Organization (BMDOLINK)
      - Defense Advanced Research Projects Agency (DARPA)
      - Defense Commissary Agency (DeCA)
      - Defense Contract Audit Agency (DCAA)
      - Defense Finance and Accounting Service (DFAS)
      - Defense Information Systems Agency (DISA)
      - Defense Intelligence Agency (DIA)
      - Defense Legal Services Agency
      - Defense Logistics Agency (DLA)
        - Corporate Administration
          - DLA Environmental and Safety Policy Office (CAAE)
          - Defense Automatic Addressing System Center (DAASC)
          - DLA Office of Operations Research and Resource Analysis (DORRA)
        - Chief Information Officer
          - Defense Systems Design Center (DSDC)
        - Defense Automated Printing Service Center
          - Defense Automated Printing Service
            - Index of Specifications and Standards (DoDISS)
            - Single Stock Point for Specifications and Standards (DoDSSP)
          - Defense Administrative Support Center
        - Defense Contract Management Command (DCMC)
          - Defense Contract Management District East (DCMDE)
          - Defense Contract Management District International (DCMDI)

U.S. Federal Government Agencies

- Defense Contract Management District West (DCMDW)
- Defense Logistics Support Command (DLSC)
  - Automatic Identification Technology Office
  - Inventory Control Points
    - Defense Energy Support Center (DESC)
    - Defense Industrial Supply Center (DISC)
    - Defense Supply Center Columbus (DSCC)
    - Defense Supply Center Richmond (DSCR)
    - Defense Supply Center Philadelphia (DSCP)
  - Defense Distribution Center (DDC)
  - Service Centers
    - Defense Reutilization and Marketing Service (DRMS)
    - Defense Logistics Information Service (DLIS)
    - Defense National Stockpile Center (DNSC)
    - Defense Distribution Systems Center (DDSC)
- Defense Security Assistance Agency
- Defense Security Service (DSS) (formerly Defense Investigative Service)
- Defense Special Weapons Agency
- Defense Technical Information Center (DTIC)
- National Imagery and Mapping Agency (NIMA)
- National Security Agency/Central Security Service
- On-Site Inspection Agency (OSIALink)

Department of Defense Field Activities

- American Forces Information Service
- Defense Medical Programs Activity
- Defense Prisoner of War/Missing Personnel Office
- Defense Technology Security Administration
- Department of Defense Human Resources Field Activity
  - Defense Civilian Personnel Management Service (CPMS)
  - Defense Manpower Data Center (DMDC)
- Department of Defense Education Activity
- Office of Civilian Health and Medical Program of the Uniformed Services
- Office of Economic Adjustment
- TRICARE Management Activity
- Washington Headquarters Services

Unified Commands

- U.S. European Command, Stuttgart-Vaihingen, Germany
- U.S. Pacific Command, Honolulu, HI
- U.S. Atlantic Command, Norfolk, VA
- U.S. Southern Command, Miami, FL
- U.S. Central Command, MacDill Air Force Base, FL
- U.S. Space Command, Peterson Air Force Base, CO
- U.S. Special Operations Command, MacDill Air Force Base, FL
- U.S. Transportation Command, Scott Air Force Base, IL
- U.S. Strategic Command, Offutt Air Force Base, NE

Coast Guard (in time of war)

- Commandant (G-C)
  - Master Chief Petty Officer of the Coast Guard

U.S. Federal Government Agencies

- Chief Administrative Law Judge for the U.S. Coast Guard
- Civil Rights Directorate (G-H)
  - Partnerships in Education
- Chief of Staff (G-CCS)
  - National Pollution Funds Center
- Acquisitions Directorate (G-A)
- Chief Counsel (G-L)
- Human Resources Directorate (G-W)
  - Reserve and Training (G-WT)
  - Personnel Management Staff (G-WP)
  - Resource Management Staff (G-WR)
  - Health and Safety Directorate(G-WH)
- Marine Safety and Environmental Protection (G-M)
- Operations Directorate (G-O)
  - U.S. Coast Guard Auxillary
  - Office of Boating Safety
  - Office of Law Enforcement
  - National Response Center
  - Navigation Center
- Systems Directorate (G-S)
  - Operations Systems Center
  - Research and Development Center
- United States Coast Guard Academy

Department of the Air Force

- Headquarters United States Air Force
- Air Combat Command
- Air Education and Training Command
- Air Force Materiel Command
- Air Force Reserve Command
- Air Force Reserve Officer Training Corps (AFROTC)
- Air Force Special Operations Command (AFSOC)
- Air Force Space Command
- Air Force Mobility Command
- Air National Guard
- Pacific Air Forces
- U.S. Air Forces in Europe
- Field Operating Agencies
  - Air Force Agency for Modeling and Simulation
  - Air Force Audit Agency
  - Air Force Base Conversion Agency
  - Air Force Center for Environmental Excellence
  - Air Force Center for Quality and Management Innovation
  - Air Force Civil Engineer Support Agency
  - Air Force Colonel Matters Office
  - Air Force Communications Agency
  - Air Force Contingency Supply Squadron
  - Air Force Flight Standards Agency
  - Air Force Historical Research Agency

U.S. Federal Government Agencies

- Air Force History Support Office
- Air Force Information Warfare Center
- Air Force Inspection Agency
- Air Force Logistics Management Agency
- Air Force Medical Logistics Office
- Air Force Medical Support Agency
- Air Force National Security Emergency Preparedness Agency
- Air Force Office of Scientific Research
- Air Force Office of Special Investigations
- Air Force Personnel Center
- Air Force Safety Center
- Air Force Services Agency
- Air Force Studies and Analyses Agency
- Air Force Technical Applications Center
- Air Force Weather Agency
- Air Force Intelligence Agency
- Air Force Reserve Personnel Center
- United States Air Force Academy

Department of the Army

- U.S. Army Corps of Engineers
  - Regional Headquarters
    - Great Lakes Regional Headquarters (CELRD-GL)
    - Ohio River Regional Headquarters (CELRD-OR)
    - Missouri River Regional Headquarters (CENWD)
    - North Pacific Regional Headquarters (CENWD-NP)
  - Divisions
    - Great Lakes and Ohio River Division (CELRD)
    - Mississippi Valley Division (CEMVD)
    - North Atlantic Division (CENAD)
    - Northwestern Division (CENWD)
    - Pacific Ocean Division (CEPOD)
    - South Atlantic Division (CESAD)
    - South Pacific Division (CESPD)
    - Southwestern Division (CESWD)
  - Laboratories
    - Cold Regions Research and Engineering Laboratory (CECRL)
    - Construction Engineering Research Laboratories(CECER)
    - Waterways Experiment Station (CEWES)
    - Topographic Engineering Center (CETEC)
- Army Digitization Office (ADO)
- Army Research Laboratory (ARL)
- U.S. Army Financial Management
- U.S. Military Academy
- White Sands Missile Range (WSMR)

Department of the Navy

- Department of the Navy Environmental Program
- Office of the Assistant Secretary of the Navy (Financial Management and Comptroller)
  - Office of Budget

U.S. Federal Government Agencies

- Office of Information
- Office of the Naval Inspector General
- Office of Naval Research (ONR)
- United States Marine Corps
  - Commandant of the Marine Corps
  - Headquarters, United States Marine Corps
    - HQMC Staff Agencies
      - Marine Corps Uniform Board
      - Administration and Resources
      - Historical Division
      - Inspector General
      - Staff Judge Advocate to the Commandant
      - Morale, Welfare and Recreation
      - Division of Public Affairs
      - Programs and Resources
      - Marine Corps Combat Development Command
      - Total Quality Leadership
      - Director, Marine Corps Staff
      - Command, Control, Communications, computer and Intelligence (C4I) Department
      - Health Services
      - Installations and Logistics Department
      - Manpower and Reserve Affairs
      - Office of Legislative Affairs
      - Plans, Policies and Operations
      - Marine Corps Systems Command
      - Marine Corps Recruiting Command
      - Safety Division
    - Marine Expeditionary Units
  - United States Naval Academy
- Joint Service Schools
  - Defense Acquisition University
  - Defense Systems Management College
  - Joint Military Intelligence College
  - National Defense University
  - National War College
    - Air War College
    - Army War College
    - Marine War College
    - Naval War College
  - Industrial College of the Armed Forces
  - Armed Forces Staff College
  - Information Resources Management College
  - Uniformed Services University of the Health Sciences
- National Guard

Department of Education

U.S. Federal Government Agencies

External Relations
Office of Intergovernmental and Interagency Affairs
Information Resource Center
Office of Non-Public Education
Partnership for Family Involvement in Education
Office of Legislation and Congressional Affairs
Operations
Office of Management
Family Policy Compliance Office
Office of Hearings and Appeals
Office of the Chief Information Officer
Office of the Chief Financial Officer
Programs
Office of Bilingual Education and Minority Languages Affairs (OBEMLA)
Office for Civil Rights
Office of Educational Research and Improvement (OERI)
National Center for Education Statistics (NCES)
National Educational Research Policy and Priorities Board
National Institute on Early Childhood Development and Education
National Institute on the Education of At-Risk Students
National Institute on Educational Governance, Finance, Policy-Making, and Management
National Institute on Postsecondary Education, Libraries, and Lifelong Learning (PLLI)
National Institute on Student Achievement, Curriculum, and Assessment
National Library of Education
National Research and Development Centers
Office of Reform Assistance and Dissemination
Office of Elementary and Secondary Education (OESE)
Office of Indian Education
Office of Migrant Education
Office of Postsecondary Education (OPE)
Office of Special Education and Rehabilitative Service
National Institute on Disability and Rehabilitation Research
Rehabilitation Services Administration
Office of Special Education Programs
Office of Vocational and Adult Education (OVAE)
Regional Offices

Department of Energy
Programs and Offices
Columbus Environmental Management Project
Energy Efficiency and Renewable Energy Network
Energy Information Administration
Energy Sciences Network (ESnet)
Environment, Safety and Health
Environmental Management
Federal Energy Regulatory Commission
Fusion Energy Sciences Program

U.S. Federal Government Agencies

- Human Resources and Administration
- Oakland Operations Office
- Office of the Chief Financial Officer
- Office of Civilian Radioactive Waste Management
- Office of Defense Programs
- Office of the Departmental Representative to the Defense Nuclear Facilities Safety Board (DNFSB)
- Office of Economic Impact and Diversity
- Office of Energy Research
- Office of Field Management
- Office of Fissile Materials Disposition
- Office of Fossil Energy
- Office of General Counsel
- Office of Hearings and Appeals
- Office of Inspector General
- Office of Nonproliferation and National Security
- Office of Policy and International Affairs
- Office of Nuclear Energy, Science, and Technology
- Office of Procurement and Assistance Management
- Office of Scientific and Technical Information
- Office of the Secretary of Energy Advisory Board
- Office of Worker and Community Transition

Laboratories and Facilities

- Argonne National Laboratory (ANL)
- Brookhaven National Laboratory
- Thomas Jefferson National Accelerator Facility (formerly Continuous Electron Beam Accelerator Facility (CEBAF))
- Energy Efficiency and Renewable Energy Network (EREN)
- Fermi National Accelerator Laboratory (Fermilab)
- Hanford Site (Richland Operations Office)
- Idaho National Engineering and Environmental Laboratory (INEEL)
- Kansas City Plant
- Lawrence Berkeley Laboratory (LBL)
- Lawrence Livermore National Laboratory
  - National Energy Research Supercomputer Center
- Los Alamos National Laboratory (LANL)
  - Advanced Computing Laboratory
- National Renewable Energy Laboratory
- Nevada Operations Office
- Oak Ridge National Laboratories
  - Center for Computational Sciences
- Pacific Northwest National Laboratory (PNL)
  - William R. Wiley Environmental Molecular Sciences Laboratory
- Princeton Plasma Physics Laboratory
- Sandia National Laboratories
- Savannah River Operations Office
- Stanford Linear Accelerator Center (SLAC)

U.S. Federal Government Agencies

- Department of Health and Human Services
  - Administration on Aging
  - Administration for Children and Families
  - Health Care Financing Administration
  - Public Health Service (PHS)
    - Agency for Toxic Substances and Disease Registry
      - Case Studies in Environmental Medicine
    - Centers for Disease Control and Prevention (CDC)
      - National Center for Chronic Disease Prevention and Health Promotion
      - National Center for Environmental Health
      - National Center for Health Statistics
      - National Center for Infectious Diseases
      - National Center for Injury Prevention and Control
      - National Institute for Occupational Safety and Health
        - Mining Health & Safety Research Program
      - Epidemiology Program Office
      - International Health Program Office
      - Public Health Practice Program Office
      - National Immunization Program Childhood Immunization Initiative
    - Food and Drug Administration (FDA)
      - National Center for Food Safety and Applied Nutrition (CFSAN)
      - National Center for Toxicological Research (NCTR)
    - Indian Health Service (IHS)
    - National Institutes of Health (NIH)
      - Advanced Laboratory Workstation Project
      - Division of Computer Research and Technology (DCRT)
        - BioInformatics Molecular Analysis Section (BIMAS)
          - BioMagResBank Database Gateway
          - GenoBase Database Gateway
      - Center for Scientific Review (CSR) (formerly Division of Research Grants)
      - National Cancer Institute (NCI)
        - CancerNet
      - National Human Genome Research Institute (NHGRI)
      - National Center for Research Resources (NCRR)
      - National Eye Institute
      - National Heart, Lung and Blood Institute (NHLBI)
      - National Institute for Allergy and Infectious Diseases (NIAID)
      - National Institute of Child Health and Human Development
      - National Institute of Diabetes and Digestive and Kidney Disease (NIDDK)
      - National Institute of Drug Abuse
      - National Institute of Environmental Health Sciences (NIEHS)
      - National Institute of General Medical Sciences (NIGMS)
      - National Institute of Mental Health (NIMH)
      - National Institute of Neurological Disorders and Stroke (NINDS)
      - National Institute of Nursing Research
      - National Institute on Aging
      - National Library of Medicine (NLM)
        - National Center for Biotechnology Information (NCBI) at NLM

U.S. Federal Government Agencies

Substance Abuse and Mental Health Services Administration

Department of Housing and Urban Development (HUD)
- Office of the Secretary
  - Administrative Law Judges
  - Board of Contract Appeals
  - Chief Information Officer
  - Departmental Equal Employment Opportunity
  - Office of Departmental Operations and Coordination
  - Office of Federal Housing Enterprise Oversight
  - Office of Labor Relations
  - Office of Lead Hazard Control
  - Office of Small and Disadvantaged Business Utilization
  - Office of Special Actions
- Secretary's Representatives
- Headquarters Program Offices
  - Government National Mortgage Association (Ginnie Mae)
  - Office of Community Planning and Development
  - Office of Fair Housing and Equal Opportunity
  - Office of Housing/Federal Housing Authority (FHA)
  - Office of Public and Indian Housing
- Headquarters Support Offices
  - Office of Administration
  - Office of the Chief Financial Officer
  - Office of Congressional and Intergovernmental Relations
  - Office of General Counsel
  - Office of Policy Development and Research
  - Office of Public Affairs
- Office of Inspector General
- Local Offices

Department of the Interior
- Secretary of the Interior
- Office of the Secretary
  - Deputy Secretary
  - Executive Secretariat
  - Office of Legislative and Congressional Affairs
  - Office of Communications
  - Office of the Solicitor
  - Office of Inspector General
  - Office of the Special Trustee for American Indians
  - Office of Policy, Management and Budget
    - Human Resources
      - Office of Personnel
      - Office of Ethics
      - Office of National Service and Educational Partnerships
    - Office of Aircraft Services

U.S. Federal Government Agencies

- Office of Acquisition and Property Management
- Office of the Budget
- Office of Environmental Policy and Complianace
- Office of Financial Management
- Office of Hearings and Appeals
- Office of Insular Affairs
- Office of International Affairs
- Office of Managing Risk and Public Safety
- Office of Small and Disadvantaged Business Utilization
- Office of Information Resources Management

Assistant Secretary--Fish and Wildlife and Parks

- National Park Service (ParkNet)
  - National Park Service NatureNet
  - Air Resources Division
  - American Indian Liason Office
  - Geological Resources Division
  - Water Resources Division
- U.S. Fish and Wildlife Service
  - Air Quality Branch
  - Division of Contracting and General Services
  - Division of Endangered Species
  - Division of Environmental Contaminants
  - Division of Federal Aid
    - Fish and Wildlife Reference Service
    - Management Assistance Team
  - Division of Finance
  - Division of Habitat Conservation
    - Coastal Habitat Conservation Programs
    - National Wetlands Inventory
  - Division of Information Resources Management
    - FWS Data Administration
    - Geographic Information Systems and Spatial Data
  - Division of Law Enforcement
    - US Fish and Wildlife Forensics Lab, Ashland, Oregon
  - Division of Policy and Directives Management
  - Division of Realty
  - Federal Duck Stamp Office
    - Federal Junior Duck Stamp Conservation and Design Program
  - Fire Management
  - National Conservation Training Center
  - National Wildlife Refuge System
  - North American Waterfowl and Wetlands Office
  - Office for Human Resources
  - Office of International Affairs
  - Office of Miratory Bird Management
  - Washington Office Fisheries
  - Regions
    - Region 1 (Pacific Region)

U.S. Federal Government Agr ies

- Region 2 (Southwest Region)
- Region 3 (Great Lakes-Big Rivers Region)
- Region 4 (Southeast Region)
- Region 5 (Northeast Region)
- Region 6 (Mountain-Prairies Region)
- Region 7 (Alaska Region)

Assistant Secretary--Indian Affairs
- Bureau of Indian Affairs (BIA)
  - Branch of Acknowledgement and Research
  - Office of Congressional and Legislative Affairs
  - Office of Indian Education Programs
  - Office of Tribal Services
  - Office of Trust Responsibilities
    - Division of Energy and Mineral Resources
    - Division of Forestry
    - Geographic Data Service Center
  - Office of American Indian Trust (OAIT)
    - Office of Self-Governance

Assistant Secretary--Land and Minerals Management
- Bureau of Land Management (BLM)
  - National Applied Resource Sciences Center
  - National Business Center
  - National Human Resource Management Center (NHRMC)
  - National Information Resource Management Center
  - National Interagency Fire Center
  - National Training Center
  - National Wild Horse and Burro Program
  - State Offices
- Minerals Management Service
  - Environmental Studies Program Information System
  - Offshore Minerals Management Program (OMM)
  - Royalty Management Program
- Office of Surface Mining Reclamation and Enforcement

Assistant Secretary--Water and Science
- Bureau of Reclamation
  - Acquisition and Assistance Management Services
  - Denver Administrative Service Center
  - Human Resources Center
  - Management Service Office
  - Program Analysis Office
  - Reclamation Services Center
  - Technical Service Center
  - Regional Offices
    - Great Plains Region
    - Lower Colorado Region
    - Mid-Pacific Region
    - Pacific Northwest Region
    - Upper Colorado Region

U.S. Federal Government Agencies

U.S. Geological Survey (USGS)

Department of Justice (DOJ)
- Office of the Attorney General
  - Office of the Deputy Attorney General
    - Office of the Solicitor General
    - Office of the Associate Attorney General
    - Community Relations Service
    - Executive Office for United States Trustees
    - Foreign Claims Settlement Commission
    - Office of Community Oriented Policing Services (COPS)
    - Office of Dispute Resolution
    - Office of Information and Privacy
    - Office of Justice Programs
      - Program Offices
        - American Indian and Alaska Native Affairs Desk
        - Corrections Program Office
        - Drug Courts Program Office
        - Executive Office for Weed and Seed
        - Violence Against Women Grants Office
        - Violence Against Women Office
      - Bureaus
        - Bureau of Justice Assistance
        - Bureau of Justice Statistics
        - National Institute of Justice
          - Crime Mapping Research Center
          - National Criminal Justice Reference Service
            - Justice Information Center
          - Office of Science and Technology
            - National Law Enforcement and Corrections Technology Center (JustNet)
        - Office of Juvenile Justice and Delinquency Prevention
        - Office for Victims of Crime
          - Federal Crimes Victims Division
          - State Compensation and Assitance Division
          - Special Projects Division
      - Support Offices
        - Equal Employment Opportunity Office
        - Office of Administration
        - Office of Budget and Management Services
        - Office for Civil Rights
        - Office of the Comptroller
        - Office of Congressional and Public Affairs
        - Office of General Counsel
    - Antitrust Division
    - Civil Division
    - Civil Rights Division

U.S. Federal Government Agencies

- Environment and National Resources Division
- Tax Division
- Office of Intergovernmental Affairs
- Office of Legal Counsel
- Office of Legislative Affairs
- Office of Policy Development
- Office of Public Affairs
- Bureau of Prisons
  - National Institue of Corrections
- Criminal Division
- Drug Enforcement Administration (DEA)
- Executive Office for United States Attorneys
  - United States Attorneys
- Federal Bureau of Investigation (FBI)
  - FBI Academy
  - FBI Laboratory
  - Field Offices
  - National Computer Crime Squad
  - National Infrastructure Protection Center (NIPC)
- Immigration and Naturalization Service (INS)
- United States Marshals Service
- United States National Central Bureau (USNCB)--INTERPOL
- Executive Office for Immigration Review
- Justice Management Division
- National Drug Intelligence Center
- Office of the Inspector General
- Office of Intelligence Policy and Review
- Office of the Pardon Attorney
- Office of Professional Responsibility
- United States Parole Commission

Department of Labor (DOL)

- Office of the Secretary
- Office of the Assistant Secretary for Administration and Management
- Office of the Assistant Secretary for Policy
- Office of the Chief Financial Officer
- Office of the Chief Information Officer
- Office of the Inspector General
- Office of the Solicitor
- Administrative Review Board
- Benefits Review Board
- Bureau of International Labor Affairs
- Bureau of Labor Statistics
- Employees' Compensation Appeals Board (ECAB)
- Employment and Training Administration
- Employment Standards Administration
  - Office of Federal Contract Compliance Programs

U.S. Federal Government Agencies

- Office of Labor-Management Standards
- Office of Workers' Compensation Programs
  - Division of Federal Employees' Compensation
  - Division of Coal Mine Workers' Compensation
  - Division of Longshore and Harbor Workers' Compensation
- Wage and Hour Division

Mine Safety and Health Administration
- Directorate of Educational Policy and Development
  - National Mine Health and Safety Academy
- District Offices

Occupational Safety and Health Administration (OSHA)
Office of Administrative Law Judges
Office of Small Business Programs
Pension and Welfare Benefits Administration
Veterans' Employment and Training Service
Women's Bureau

Department of State
- Secretary of State
  - Operations Center
  - Policy Planning Staff
  - Office of Resources, Plans and Policy
  - Office of the Chief of Protocol
  - Office of the Permanent Representative to the United Nations
  - Bureau of Public Affairs
    - Office of the Historian
  - Bureau of Legislative Affairs
  - Bureau of Intelligence and Research
  - Office of Inspector General
  - Office of the Legal Adviser
- Office of Under Secretary for Political Affairs
  - Geographic Bureaus
    - Bureau of African Affairs
    - Bureau of East Asian and Pacific Affairs
    - Bureau of European and Canadian Affairs
    - Bureau of Inter-American Affairs
    - Breau of Near Eastern Affairs
    - Bureau of South Asian Affairs
    - Office of the Special Adviser to the Secretary for the New Independent States
  - Bureau of International Organization Affairs
- Office of Under Secretary for Economic, Business, and Agricultural Affairs
  - Office of the Coordinator for Business Affairs
  - Bureau of Economic and Business Affairs
- Office of Under Secretary for Arms Control and International Security Affairs
  - Bureau of Political Military Affairs
    - Office of Defense Trade Controls
    - Nonproliferation and Disarmament Fund

U.S. Federal Government Agencies

- Office of Under Secretary for Management
  - Office of Foreign Missions
  - Foreign Service Institute
  - Director General of Foreign Service and Director of Personnel
    - Family Liason Office
  - Bureau of Administration
    - Office of Allowances
    - Office of Overseas Schools
    - Office of the Procurement Executive
    - Office of Small and Disadvantaged Business Utilization
    - Ralph J. Bunche Library
  - Bureau of Consular Affairs
  - Bureau of Diplomatic Security
    - Overseas Security Advisory Council (OSAC)
  - Bureau of Finance and Management Policy
- Office of Under Secretary for Global Affairs
  - Bureau of Democracy, Human Rights, and Labor
  - Bureau for International Narcotics and Law Enforcement Affairs
  - Bureau of Oceans and International Environmental and Scientific Affairs
  - Bureau of Population, Refugees, and Migration
  - Office of the Coordinator for Counterterrorism
  - Office of the Senior Coordinator for International Women's Issues
- U.S. Missions Online
- Office of Authentication

- Department of Transportation
  - Office of the Secretary
  - Bureau of Transportation Statistics
  - Coast Guard (in time of peace)
  - Federal Aviation Administration (FAA)
    - Associate Administrator for Administration
    - Associate Administrator for Commercial Space Transportation
    - Civil Aviation Security
    - Office of the Associate Administrator for Airports
    - Office of System Safety
    - Flight Standards Service
    - Mike Monroney Aeronautical Center
    - William J. Hughes Technical Center
  - Federal Highway Administration
    - Associate Administrator for Policy
      - Office of International Programs
      - Office of Policy Development
      - Office of Highway Information Management
    - Associate Administrator for Research and Development
      - Turner-Fairbank Highway Research Center
      - Office of Research and Development Operations and Support
      - Office of Engineering Research and Development

U.S. Federal Government Agencies

- Office of Safety and Traffic Operations Research and Development
  - Traffic and Driver Information Systems Division
- Associate Administrator for Motor Carriers
- Office of Administration
- Office of Program Development
- Federal Railroad Administration
- Federal Transit Administration
- National Highway Traffic Safety Administration (NHTSA)
- Maritime Administration
- National Transportation Library
- Research and Special Programs Administration
- Saint Lawrence Seaway Development Corporation
- Surface Transportation Board
- Transportation Administrative Service Center (TASC)

Department of the Treasury

- Treasury Bureaus
  - Internal Revenue Service (IRS)
  - United States Customs Service
  - Bureau of Alcohol, Tobacco, and Firearms
  - Financial Management Service
  - United States Secret Service
  - Office of Thrift Supervision
  - United States Mint
  - Office of the Comptroller of the Currency
  - Federal Law Enforcement Training Center
  - Bureau of the Public Debt
  - Bureau of Engraving and Printing
  - Financial Crimes Enforcement Network
  - Community Development Financial Institutions Fund
- Treasury Offices
  - Office of Domestic Finance
  - Office of Economic Policy
    - Foreign Investment Survey
  - Office of Enforcement
  - Office of International Affairs
  - Office of Legislative Affairs
  - Office of Management
    - Chief Information Officer
    - Chief Financial Officer
    - Office of Equal Opportunity Program
    - Government Information Technology Services (GITS)
    - GITS Security
    - Office of Small and Disadvantaged Business Utilization
    - Office of Treasury Reinvention
    - Office of Budget

U.S. Federal Government Agencies

Department of Veterans Affairs
- Board of Contract Appeals
- Board of Veterans' Appeals
- Chief Information Officers Council
- Inter-Agency Benchmarking and Best Practices Council
- National Cemetery System (NCS)
- Office of Acquisition and Materiel Management
- Office of Congressional Affairs
- Office of Financial Management
- Office of Information Resources Management
- Office of Inspector General
- Office of Occupational Safety and Health
- Office of Small and Disadvantaged Business Utilization
- Veterans Health Administration (VHA)
  - Diabetes Program
  - National Center for Health Promotion and Disease Prevention
  - National Chaplain Center
  - Nursing Service
  - Office of Research and Development
  - Physical Medicine and Rehabilitation Service
  - Veterans Integrated Service Networks
- Veterans Benefits Association (VBA)
  - Debt Management Center
  - Compensation and Pension Service
  - Education Service
  - Insurance Service
  - Loan Guaranty Service
  - Vocational Rehabilitation and Counseling Service

Executive	Judicial	Legislative	Independent	Boards, Commissions, and Committees	Quasi-Official

Judicial Branch

Administrative Office of the U.S. Courts (Federal Judiciary Homepage)
Federal Judicial Center
United States Sentencing Commission

United States Supreme Court
- Supreme Court via LII at Cornell Law School (opinions since 1990 and selected historical decisions)
- Supreme Court via FindLaw (opinions since 1893)
- Supreme Court via Oyez Oyez Oyez (Real Audio recordings of oral arguments)

Courts of Appeal (see also U.S. Federal Courts Finder)
- First Circuit
  - First Circuit via Emory University School of Law (opinions since November 1995)
  - First Circuit via FindLaw (opinions since November 1995)
- Second Circuit
  - Second Circuit via Touro Law Center (opinions since January 1995)

U.S Federal Government Agencies

Second Circuit via Pace University School of Law (opinions since September 1995)
Second Circuit via FindLaw (opinions since January 1995)

Third Circuit
Third Circuit via Villanova Center for Information Law and Policy (opinions since May 1994)
Third Circuit via FindLaw (opinions since May 1994)

Fourth Circuit
Fourth Circuit via Emory University School of Law (opinions since January 1995)
Fourth Circuit via FindLaw (opinions since January 1995)

Fifth Circuit
Official Fifth Circuit Web Site (opinions since 1991, other documents, general information)
Fifth Circuit via FindLaw (recent opinions only)

Sixth Circuit
Sixth Circuit via Emory University School of Law (opinions since January 1995)
Sixth Circuit via FindLaw (opinions since January 1995)

Seventh Circuit
Seventh Circuit via Chicago-Kent College of Law (opinions since January 1993)
Seventh Circuit via FindLaw (opinions since June 1995)

Eighth Circuit
Eighth Circuit via Washington University School of Law (opinions since November 1995)
Eighth Circuit via FindLaw (opinions since November 1995)

Ninth Circuit
Office of the Circuit Executive--Official Ninth Circuit Web Site (general information; no opinions available)
Ninth Circuit via Villanova Center for Information Law and Policy (opinions since June 1995)
Ninth Circuit via FindLaw (opinions since 1990)

Tenth Circuit
Tenth Circuit Clerk--Official Tenth Circuit Web Site (general information: no opinions available)
Tenth Circuit via Emory University School of Law (opinions from August 1995 to October 1997)
Tenth Circuit via Washburn University School of Law (opinions since October 1997)
Tenth Circuit via FindLaw (recent opinions only)

Eleventh Circuit
Eleventh Circuit Library Reference Desk (links and general information; no opinions available)
Eleventh Circuit Internet Pilot Project (opinions from the last three months)
Eleventh Circuit via Emory University School of Law (opinions since November 1994)
Eleventh Circuit via FindLaw (opinions since December 1994)

District of Columbia Circuit
Official D.C. Circuit Web Site (opinions since September 1997, general information)
D.C. Circuit via Georgetown University Law Center (opinions since March 1995)
D.C. Circuit via FindLaw (opinions since February 1995)

Federal Circuit
Official Federal Circuit Web Site (recent opinions only)
Federal Circuit via Emory University School of Law (opinions since August 1995)
Federal Circuit via Georgetown University Law Center (opinions since August 1995)

U.S. Federal Government Agencies

Federal Circuit via FindLaw (recent opinions only)
U.S. Court of Appeals for the Armed Forces (administratively located in the Department of Defense)
Official U.S. Court of Appeals for the Armed Forces Web Site (opinions since October 1996; general information)

Executive	Judicial	Legislative	Independent	Boards, Commissions, and Committees	Quasi-Official

Legislative Branch

U.S. House of Representatives
Representatives on the Web
U.S. House of Representatives Internet Law Library

U.S. Senate
Senators on the Web

Congressional Budget Office (CBO)
General Accounting Office (GAO)
Government Printing Office (GPO)
Institute for Federal Printing and Publishing (IFPP)
LSU Libraries GPO Access Gateway
Library of Congress
LOCIS: Library of Congress Online Public Access Catalog
LC Marvel
THOMAS: Legislative Information on the Internet
103rd Congress Bills
104th Congress Bills
105th Congress Bills
Office of Compliance
Office of Technology Assessment
Stennis Center for Public Service

Executive	Judicial	Legislative	Independent	Boards, Commissions, and Committees	Quasi-Official

Independent Establishments and Government Corporations

African Development Foundation
Central Intelligence Agency (CIA)
Intelligence Community
Commission on Civil Rights
Commodity Futures Trading Commission (CFTC)
Consumer Product Safety Commission (CPSC)
Corporation for National Service
Defense Nuclear Facilities Safety Board (DNFSB)
Environmental Protection Agency (EPA)
Equal Employment Opportunity Commission (EEOC)

U.S. Federal Government Agencies

- Export-Import Bank of the United States
- Farm Credit Administration
- Federal Communications Commission (FCC)
- Federal Deposit Insurance Corporation (FDIC)
- Federal Election Commission (FEC)
- Federal Emergency Management Agency (FEMA)
- Federal Housing Finance Board
- Federal Labor Relations Authority
- Federal Maritime Commission
- Federal Mediation and Conciliation Service
- Federal Mine Safety and Health Review Commission
- Federal Reserve System Board of Govenors
  - Federal Reserve Bank of Atlanta
  - Federal Reserve Bank of Boston
  - Federal Reserve Bank of Chicago
  - Federal Reserve Bank of Cleveland
  - Federal Reserve Bank of Dallas
  - Federal Reserve Bank of Kansas City
  - Federal Reserve Bank of Minneapolis
  - Federal Reserve Bank of New York
  - Federal Reserve Bank of Philadelphia
  - Federal Reserve Bank of San Francisco
  - Federal Reserve Bank of St. Louis
- Federal Retirement Thrift Investment Board
- Federal Trade Commission (FTC)
- General Services Administration (GSA)
  - Consumer Information Center
  - Federal Supply Service
  - Federal Technology Service (formerly Federal Telecomunications Service)
    - Office of Information Technology Integration
    - Office of Information Security
    - Federal Information Center
      - Federal Information Relay Service
      - Catalog of Federal Domestic Assistance Programs
  - Office of Governmentwide Policy
  - Public Buildings Service
- Inter-American Foundation
- Merit Systems Protection Board
- National Aeronautics and Space Administration (NASA)
  - Ames Research Center
  - Dryden Flight Research Center
  - Goddard Institute for Space Studies
  - Goddard Space Flight Center
  - Independent Validation and Verification Facility
  - Jet Propulsion Laboratory
  - Johnson Space Center
  - Kennedy Space Center
  - Langley Research Center

U S. Federal Government Agencies

- Lewis Research Center
- Marshall Space Flight Center
- Moffett Federal Airfield
- Stennis Space Center
- Wallops Flight Facility
- White Sands Test Facility

National Archives and Records Administration (NARA)
- The Center for Electronic Records

National Capital Planning Commission
National Credit Union Administration (NCUA)
National Foundation on the Arts and the Humanities
- The Institute of Museum and Library Services
- National Endowment for the Arts
  - ArtsEdge
- National Endowment for the Humanities (NEH)

National Labor Relations Board (NLRB)
National Mediation Board
National Railroad Passenger Corporation (Amtrak)
National Performance Review (NPR)
- FinanceNet

National Science Foundation (NSF)
National Transportation Safety Board
Nuclear Regulatory Commission (NRC)
Occupational Safety and Health Review Commission
Office of Government Ethics
Office of Personnel Management
Overseas Private Investment Corporation
Panama Canal Commission
Peace Corps
Pennsylvania Avenue Development Corporation
Pension Benefit Guaranty Corporation
Postal Rate Commission
Railroad Retirement Board
Resolution Trust Corporation
Securities and Exchange Commission (SEC)
- EDGAR Database

Selective Service System
Small Business Administration (SBA)
Social Security Administration (SSA)
- Regional Offices:
  - Atlanta Region
  - Boston Region
  - Chicago Region
  - Denver Region
  - Kansas City Region
  - New York Region
  - San Francisco Region
  - Seattle Region

U.S. Federal Government Agencies

Tennessee Valley Authority
Thrift Depositor Protection Oversight Board
Trade and Development Agency
United States Arms Control and Disarmament Agency
United States Information Agency (USIA)
International Broadcasting Bureau
Voice of America (VOA)
United States International Development Cooperation Agency
Agency for International Development (USAID)
The Environmental and Natural Resource Information Center
United States International Trade Commission (USITC)
United States Postal Service (USPS)

Boards, Commissions, and Committees

Administrative Committee of the Federal Register
Advisory Commission on Intergovernmental Relations
Advisory Council on Historic Preservation
American Battle Monuments Commission
Appalachian Regional Commission
Architectural and Transportation Barriers Compliance Board (Access Board)
Arctic Research Commission
Arthritis and Musculoskeletal Interagency Coordinating Committee
Barry M. Goldwater Scholarship and Excellence in Education Foundation
Citizens' Stamp Advisory Committee
Commission of Fine Arts
Committee on Foreign Investment in the United States
Committee for the Implementation of Textile Agreements
Committee for Purchase from People Who Are Blind or Severely Disabled
Coordinating Council on Juvenile Justice and Delinquency Prevention
Critical Infrastructure Assurance Office (CIAO)
Delaware River Basin Commission
Endangered Species Committee
Export Administration Review Board
Federal Financial Institutions Examination Council
Federal Financing Bank
Federal Interagency Committee on Education
Federal Interagency Council on Statistical Policy
FedStats
Federal Laboratory Consortium for Technology Transfer
Federal Library and Information Center Committee
Franklin Delano Roosevelt Memorial Commission
Harry S. Truman Scholarship Foundation
Illinois and Michigan Canal National Heritage Corridor Commission
Indian Arts and Crafts Board
Information Security Oversight Office

U.S. Federal Government Agencies

Interagency Committee on Employment of People with Disabilities
Interagency Savings Bonds Committee
J. William Fulbright Foreign Scholarship Board
James Madison Memorial Fellowship Foundation
Japan-United States Friendship Commission
Joint Board for the Enrollment of Actuaries
Marine Mammal Commission
Medicare Payment Advisory Commission (MedPAC) (formerly the Physician Payment Review Commission and the Prospective Payment Assessment Commission)
Migratory Bird Conservation Commission
Mississippi River Commission
National Commission on Libraries and Information Science
National Communications System
National Council on Disability
National Gambling Impact Study Commission
National Occupational Information Coordinating Committee
National Park Foundation
The National Park Foundation's Complete Guide to America's Parks
Northwest Power Planning Council
Office of Navajo and Hopi Indian Relocation
Office of Women's Business Ownership
Permanent Committee for the Oliver Wendell Holmes Devise
Physician Payment Review Commission
President's Committee on Employment of People with Disabilities
President's Council on Integrity and Efficiency
President's Foreign Intelligence Advisory Board
Regulatory Information Service Center
Susquehanna River Basin Commission
Textile Trade Policy Group
Trade Policy Committee
United States Holocaust Memorial Museum
United States Nuclear Waste Technical Review Board
Veterans Day National Committee
White House Commission on Presidential Scholars

Executive | Judicial | Legislative | Independent | Boards, Commissions, and Committees | Quasi-Official

Quasi-Official Agencies

Legal Services Corporation
Smithsonian Institution
Anacostia Museum
Arthur M. Sackler Gallery
Arts and Industries Building
Center for Earth and Planetary Studies (CEPS)
Cooper-Hewitt, National Design Museum
Freer Gallery of Art
Harvard-Smithsonian Center for Astrophysics

U.S. Federal Government Agencies

- Hirshhorn Museum and Sculpture Garden
- National Air and Space Museum
- National Museum of African Art
- National Museum of American Art
- National Museum of American History
- National Museum of Natural History
- National Museum of the American Indian
- National Portrait Gallery
- National Postal Museum
- National Zoo

State Justice Institute
United States Institute of Peace

Executive | Judicial | Legislative | Independent | Boards, Commissions, and Committees | Quasi-Official

---

Awards, Honors, and Recommendations Received:

LSU Libraries | LSU and Louisiana | Internet Webliography | LSU Home Page

---

Send updates and corrections to *Smittie Bolner* (sbolner@lsu.edu).

URL: http://www.lib.lsu.edu/gov/fedgov.html
Last updated: Friday, 06-Nov-98 08:49:24

Figure 11

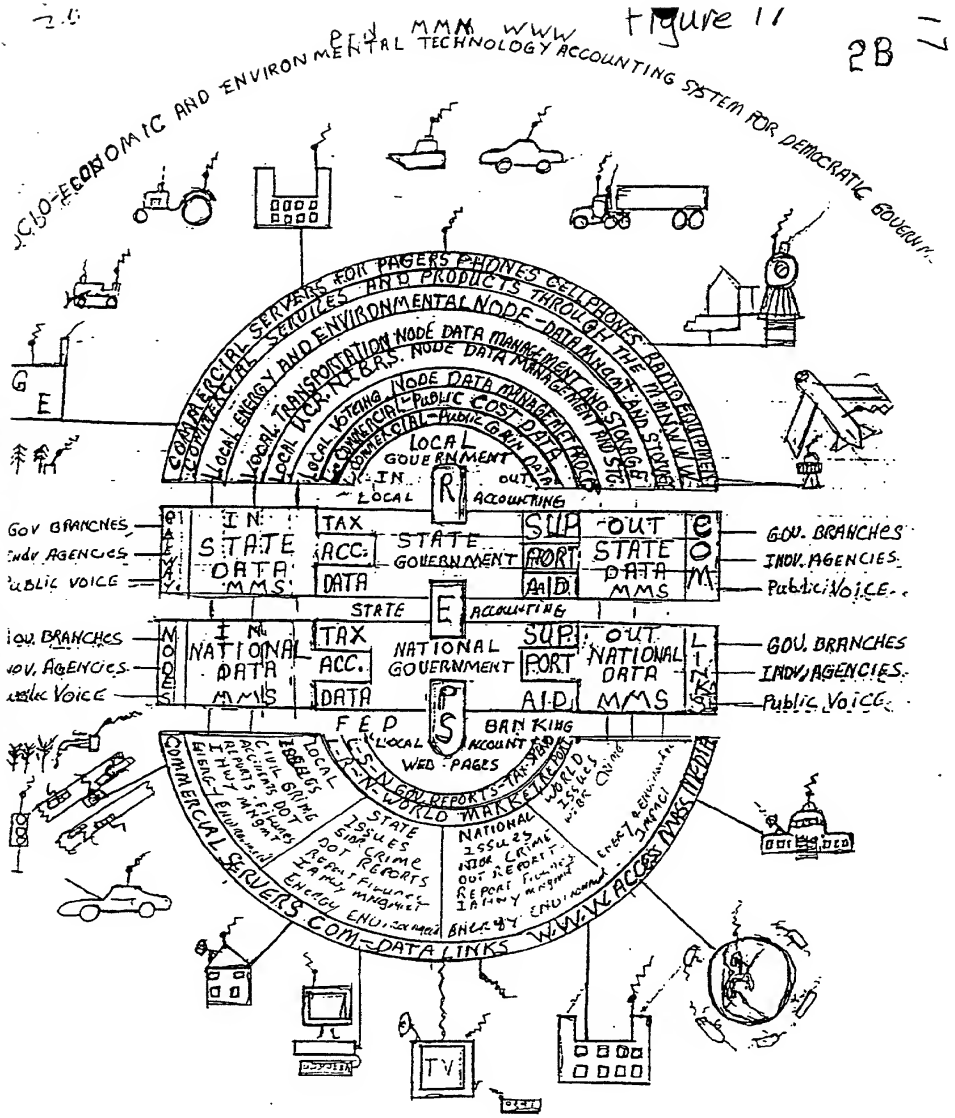

ECO-ECONOMIC AND ENVIRONMENTAL TECHNOLOGY ACCOUNTING SYSTEM FOR DEMOCRATIC GOVERN
COMMERCIAL SERVERS FOR PAGERS PHONES CELLPHONES RADIO EQUIPMENT
COMMERCIAL SERVICES AND PRODUCTS THROUGH THE INTERNET WWW
LOCAL ENERGY AND ENVIRONMENTAL NODE - DATA MANAGEMENT AND STORAGE
LOCAL TRANSPORTATION NODE DATA MANAGEMENT AND STORAGE
LOCAL VOTING NODE DATA MANAGEMENT PROCESS
COMMERCIAL - PUBLIC COST DATA
COMMERCIAL - PUBLIC GRAN DATA
LOCAL GOVERNMENT
IN - LOCAL
OUT
ACCOUNTING
GOV BRANCHES
INDV AGENCIES
PUBLIC VOICE
STATE DATA MMS
TAX ACC.
DATA
STATE GOVERNMENT
SUP PORT AID
STATE DATA MMS
GOV. BRANCHES
INDV. AGENCIES
Public Voice
STATE ACCOUNTING
NATIONAL DATA MMS
NATIONAL GOVERNMENT
NATIONAL DATA MMS
FED LOCAL ACCOUNTING
BANKING
WEB PAGES
WORLD MARKET PLACE
COMMERCIAL SERVERS.COM - DATA LINKS
WWW ACCESS NETWORKING
TV

FIG 18 FACT COMPONENT IDENITY CHIPS AND FIRMWARE MAIN SWITCH

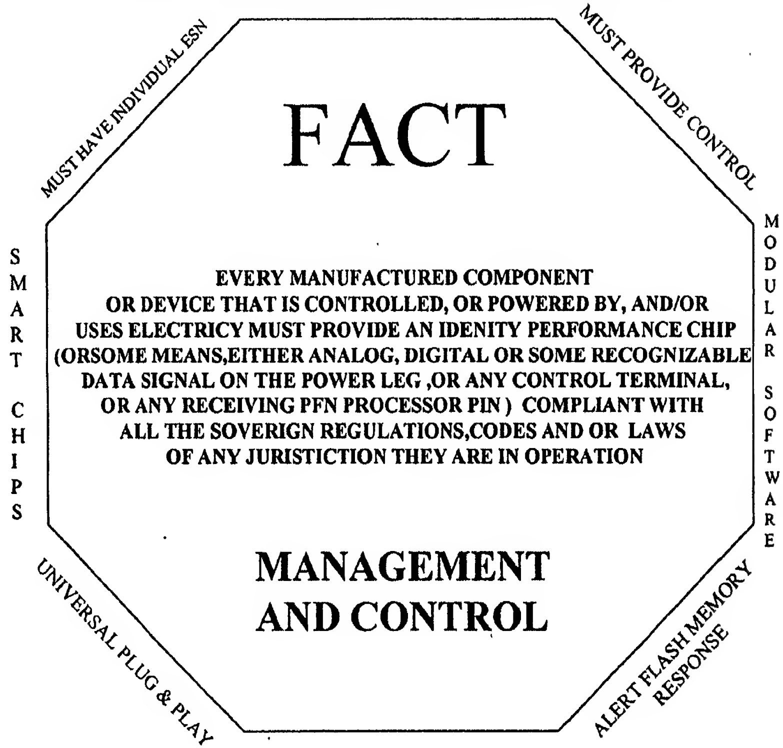


FIG 18A

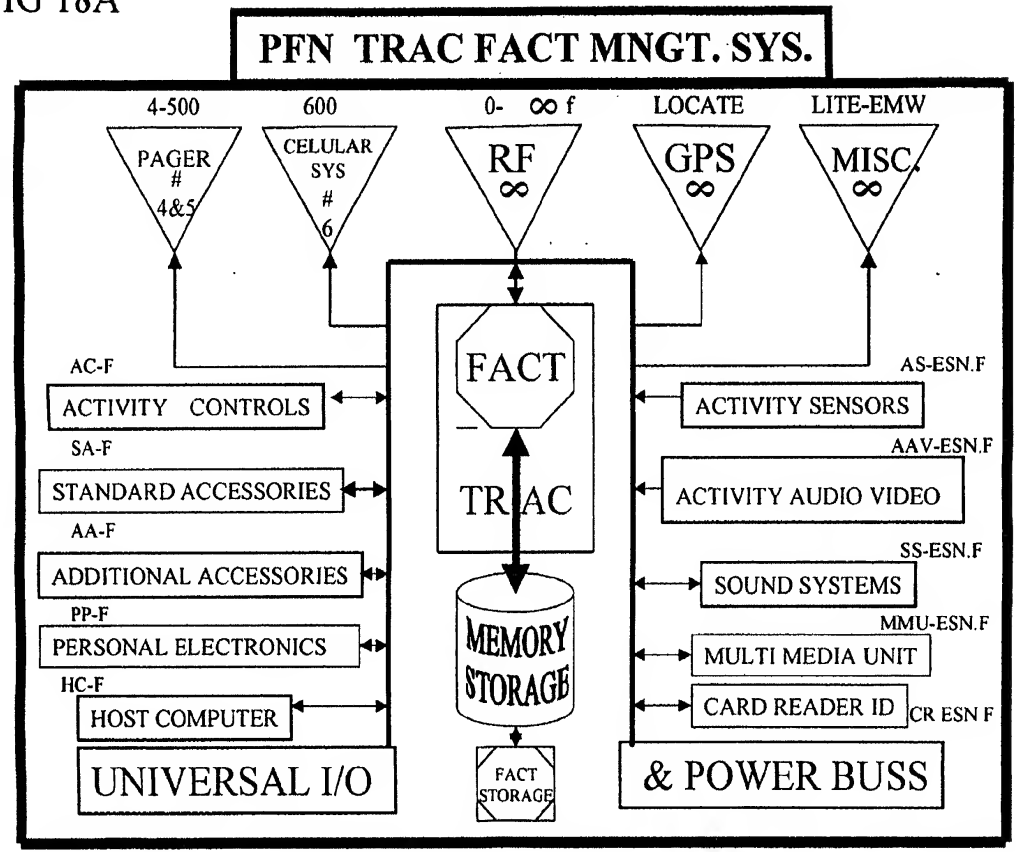

PFN TRAC FACT MNGT. SYS.
4-500
600
0- ∞ f
LOCATE
LITE-EMW
PAGER # 4&5
CELULAR SYS # 6
RF ∞
GPS ∞
MISC. ∞
FACT
TRAC
AC-F
ACTIVITY CONTROLS
SA-F
STANDARD ACCESSORIES
AA-F
ADDITIONAL ACCESSORIES
PP-F
PERSONAL ELECTRONICS
HC-F
HOST COMPUTER
UNIVERSAL I/O
MEMORY STORAGE
FACT STORAGE
AS-ESN.F
ACTIVITY SENSORS
AAV-ESN.F
ACTIVITY AUDIO VIDEO
SS-ESN.F
SOUND SYSTEMS
MMU-ESN.F
MULTI MEDIA UNIT
CARD READER ID
CR ESN F
& POWER BUSS

FIG 18B

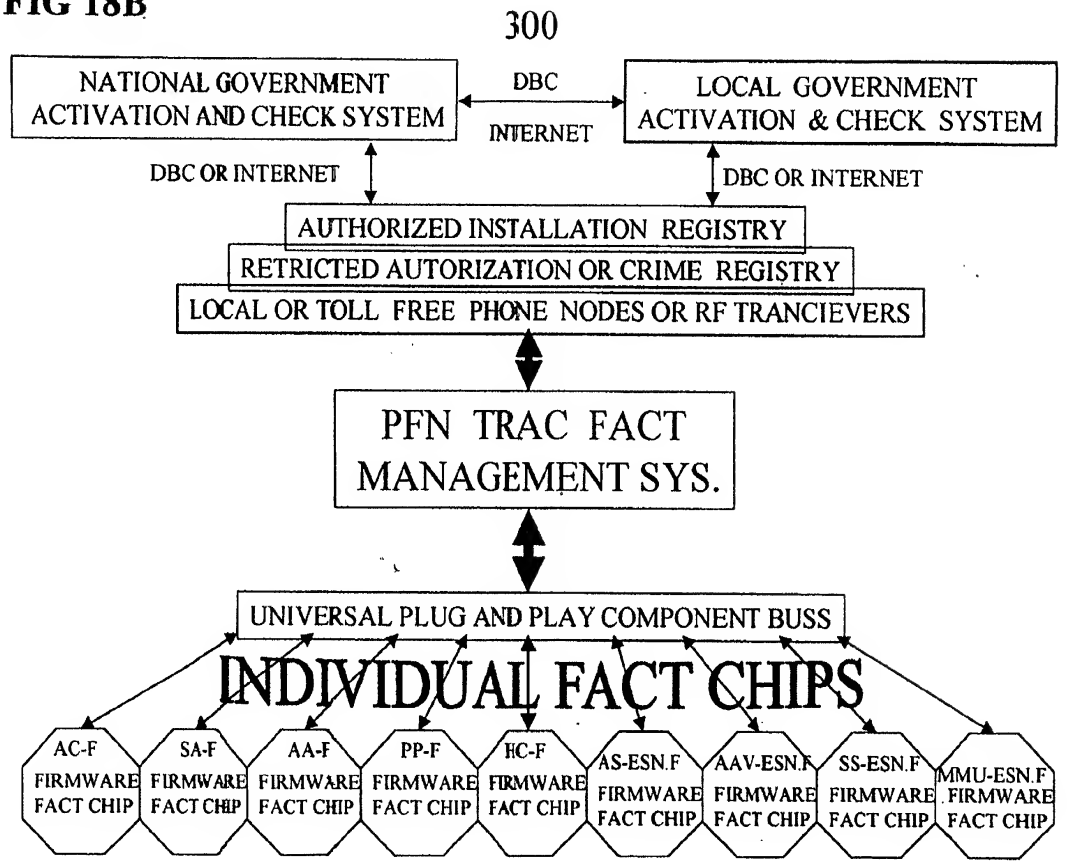


FIG 19

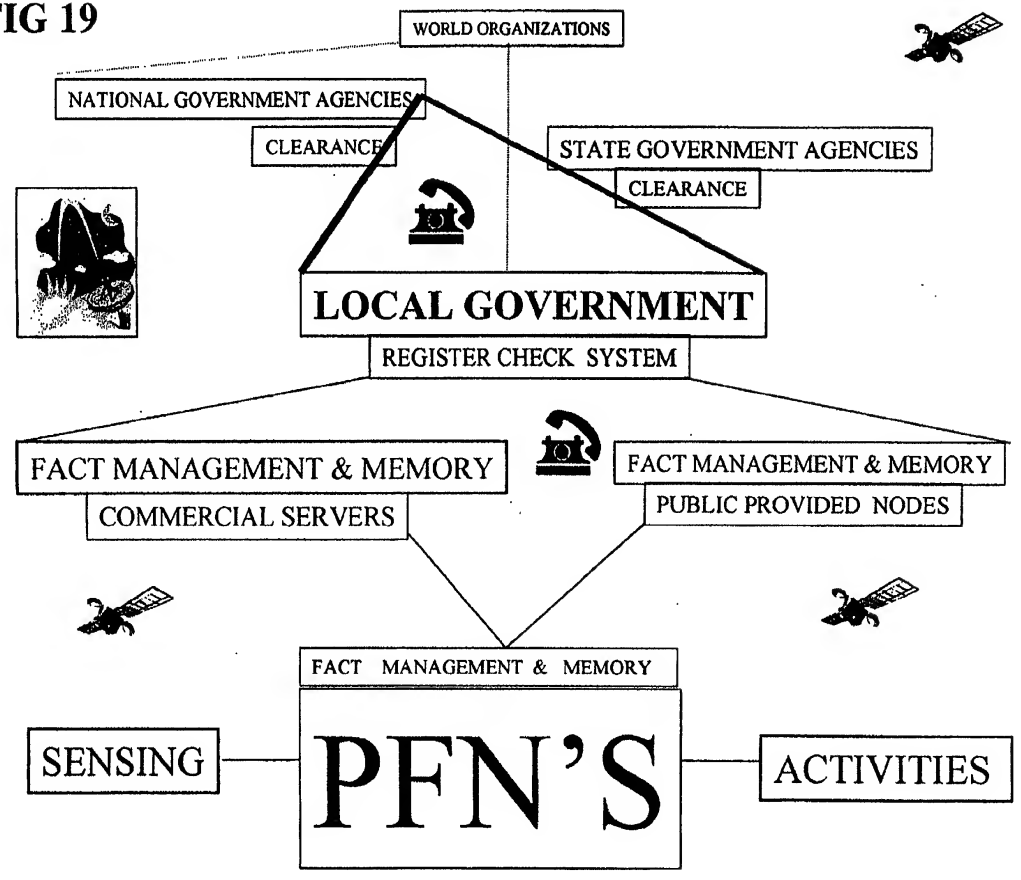


FIG 20

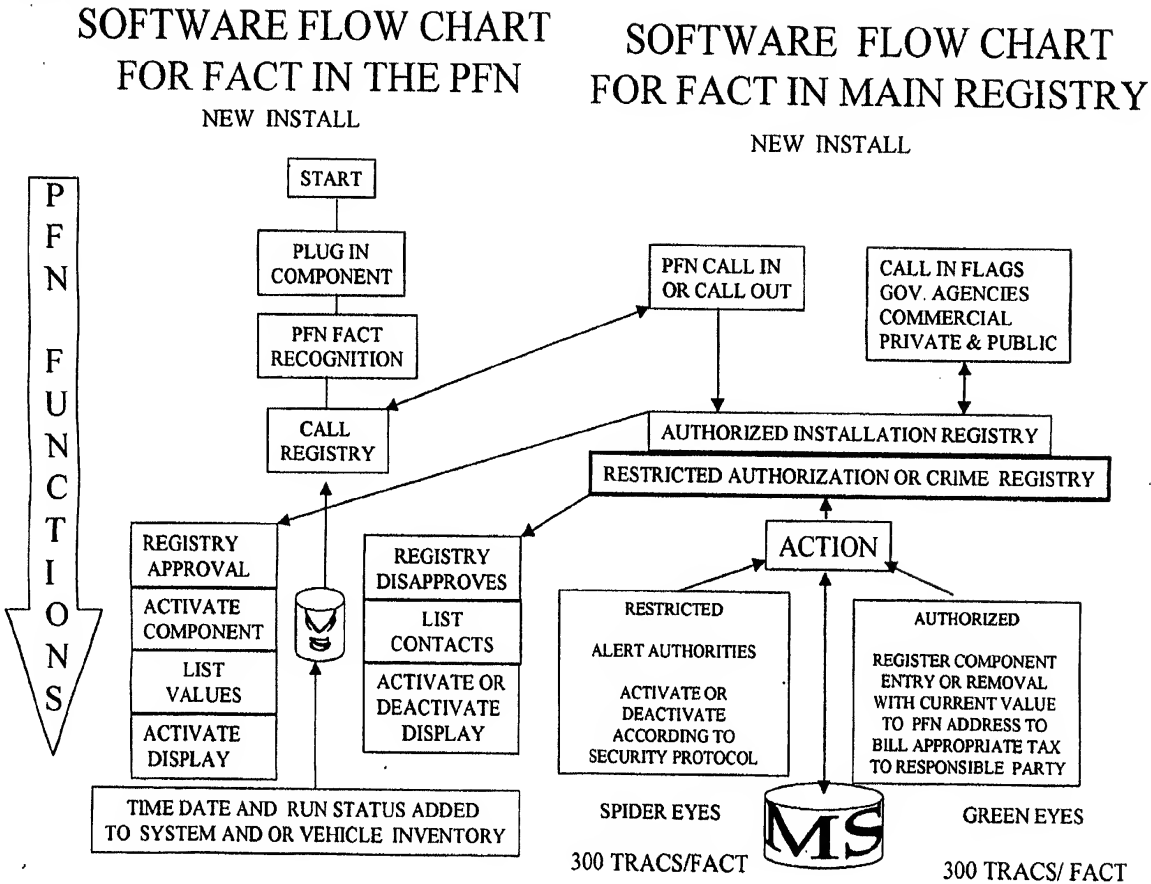

SOFTWARE FLOW CHART
FOR FACT IN THE PFN
NEW INSTALL
SOFTWARE FLOW CHART
FOR FACT IN MAIN REGISTRY
NEW INSTALL
PFN FUNCTIONS
START
PLUG IN COMPONENT
PFN FACT RECOGNITION
CALL REGISTRY
PFN CALL IN OR CALL OUT
CALL IN FLAGS
GOV. AGENCIES
COMMERCIAL
PRIVATE & PUBLIC
AUTHORIZED INSTALLATION REGISTRY
RESTRICTED AUTHORIZATION OR CRIME REGISTRY
ACTION
REGISTRY APPROVAL
ACTIVATE COMPONENT
LIST VALUES
ACTIVATE DISPLAY
REGISTRY DISAPPROVES
LIST CONTACTS
ACTIVATE OR DEACTIVATE DISPLAY
RESTRICTED
ALERT AUTHORITIES
ACTIVATE OR DEACTIVATE ACCORDING TO SECURITY PROTOCOL
AUTHORIZED
REGISTER COMPONENT ENTRY OR REMOVAL WITH CURRENT VALUE TO PFN ADDRESS TO BILL APPROPRIATE TAX TO RESPONSIBLE PARTY
TIME DATE AND RUN STATUS ADDED TO SYSTEM AND OR VEHICLE INVENTORY
SPIDER EYES
300 TRACS/FACT
MS
GREEN EYES
300 TRACS/ FACT

FIG 21

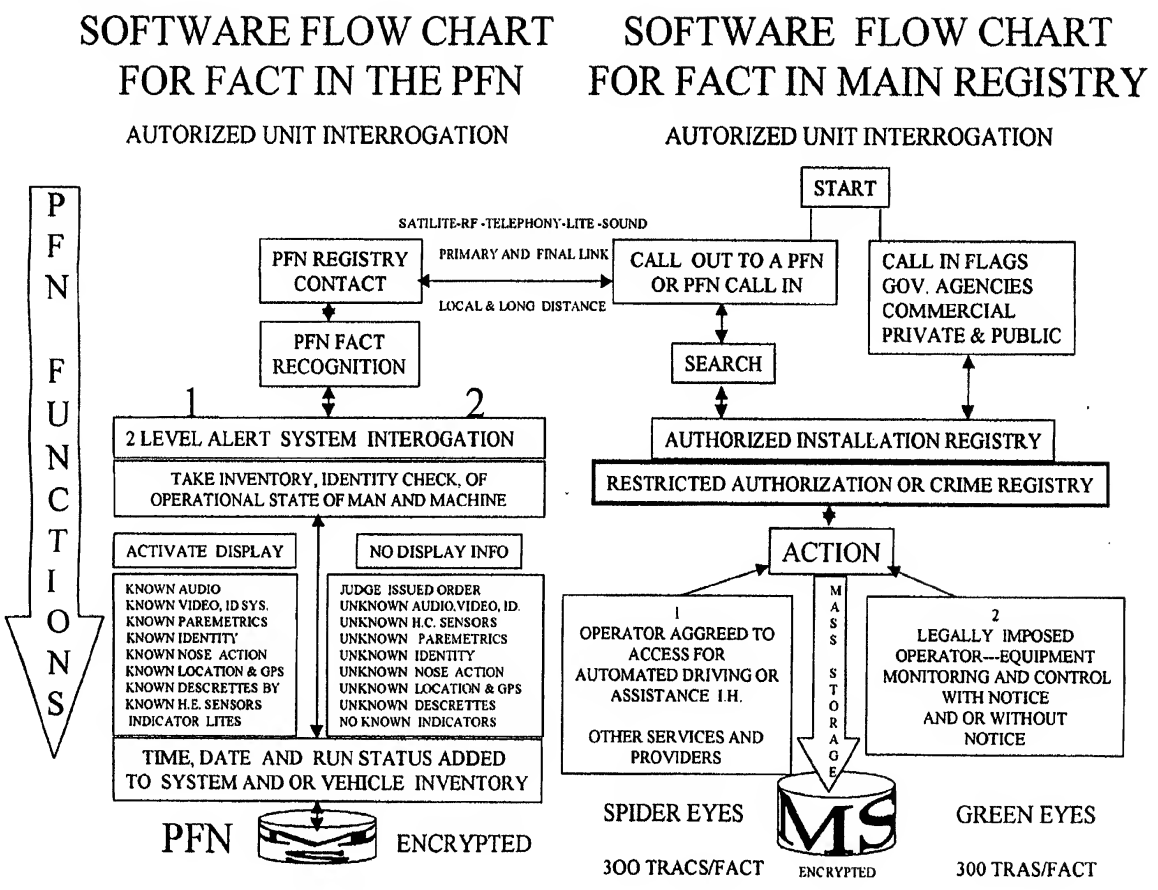
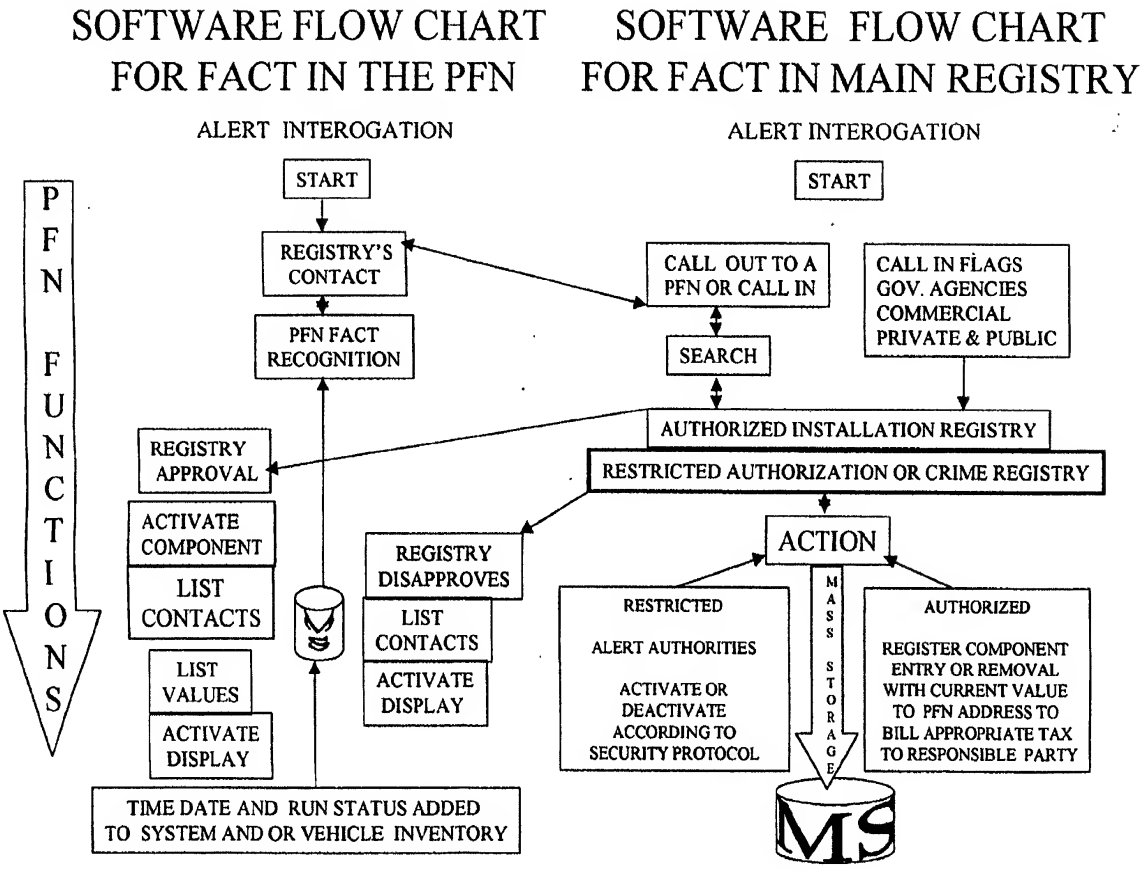

SOFTWARE FLOW CHART FOR FACT IN THE PFN
AUTORIZED UNIT INTERROGATION
SOFTWARE FLOW CHART FOR FACT IN MAIN REGISTRY
AUTORIZED UNIT INTERROGATION
PFN FUNCTIONS
SATILITE-RF -TELEPHONY-LITE -SOUND
PFN REGISTRY CONTACT
PRIMARY AND FINAL LINK
LOCAL & LONG DISTANCE
PFN FACT RECOGNITION
1
2
2 LEVEL ALERT SYSTEM INTEROGATION
TAKE INVENTORY, IDENTITY CHECK, OF OPERATIONAL STATE OF MAN AND MACHINE
ACTIVATE DISPLAY
NO DISPLAY INFO
KNOWN AUDIO
KNOWN VIDEO, ID SYS.
KNOWN PAREMETRICS
KNOWN IDENTITY
KNOWN NOSE ACTION
KNOWN LOCATION & GPS
KNOWN DESCRETTES BY
KNOWN H.E. SENSORS
INDICATOR LITES
JUDGE ISSUED ORDER
UNKNOWN AUDIO,VIDEO, ID.
UNKNOWN H.C. SENSORS
UNKNOWN PAREMETRICS
UNKNOWN IDENTITY
UNKNOWN NOSE ACTION
UNKNOWN LOCATION & GPS
UNKNOWN DESCRETTES
NO KNOWN INDICATORS
TIME, DATE AND RUN STATUS ADDED TO SYSTEM AND OR VEHICLE INVENTORY
PFN
ENCRYPTED
START
CALL OUT TO A PFN OR PFN CALL IN
CALL IN FLAGS GOV. AGENCIES COMMERCIAL PRIVATE & PUBLIC
SEARCH
AUTHORIZED INSTALLATION REGISTRY
RESTRICTED AUTHORIZATION OR CRIME REGISTRY
ACTION
1
OPERATOR AGGREED TO ACCESS FOR AUTOMATED DRIVING OR ASSISTANCE I.H.
OTHER SERVICES AND PROVIDERS
MASS STORAGE
2
LEGALLY IMPOSED OPERATOR---EQUIPMENT MONITORING AND CONTROL WITH NOTICE AND OR WITHOUT NOTICE
SPIDER EYES
300 TRACS/FACT
MS
ENCRYPTED
GREEN EYES
300 TRAS/FACT

FIG 22



wo 00/78057
55/64
10/018095
PCT/US00/16381

FIG 23 112756-501

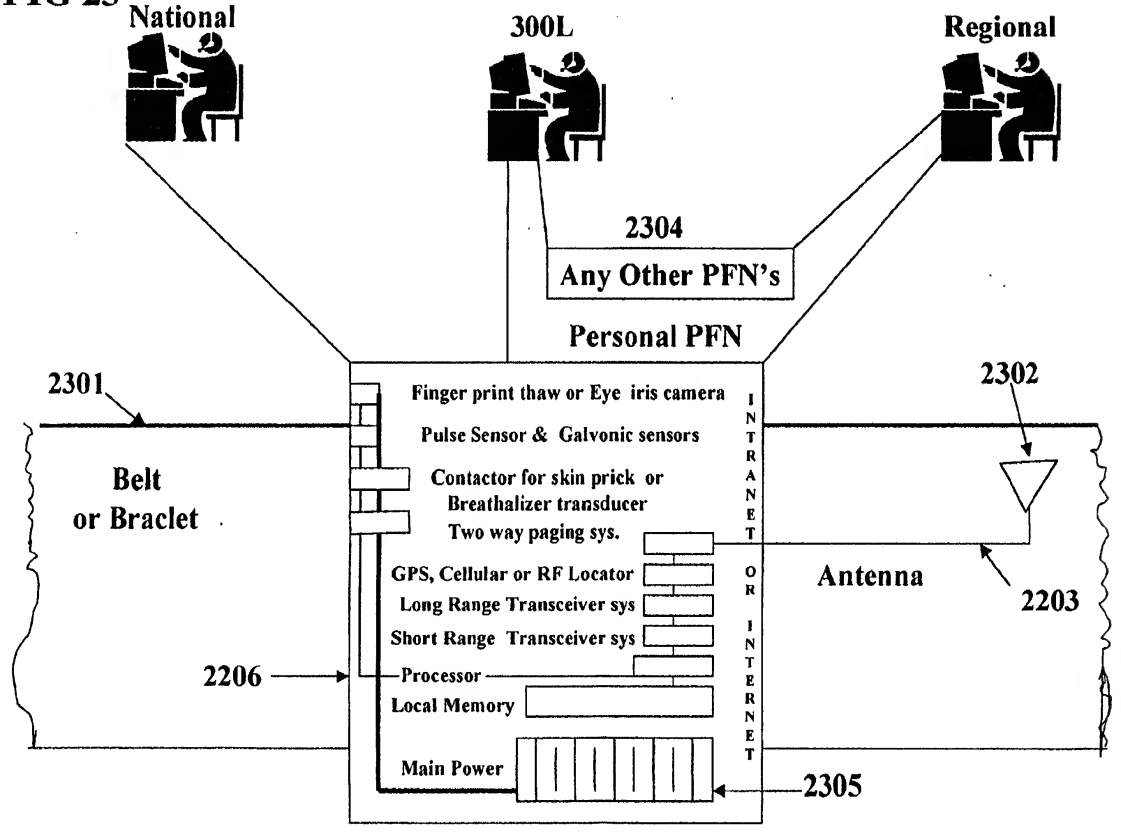


FIG. 23A RF TRACKINGFOR PERSONAL PFN'S

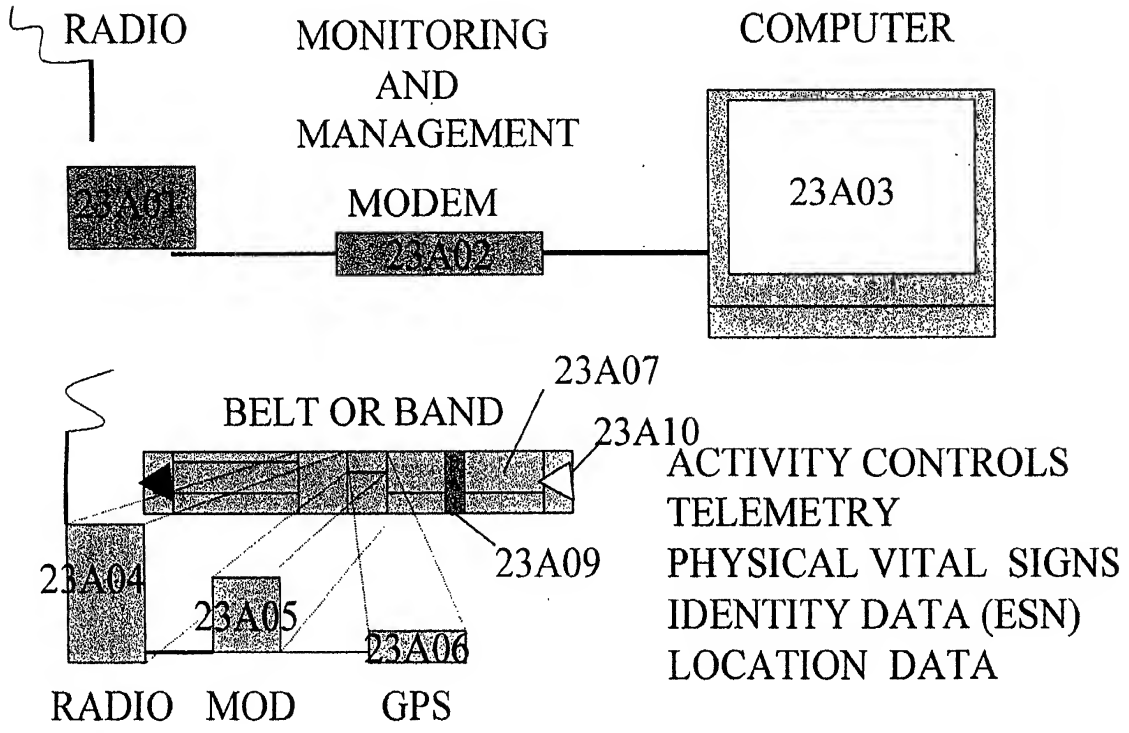
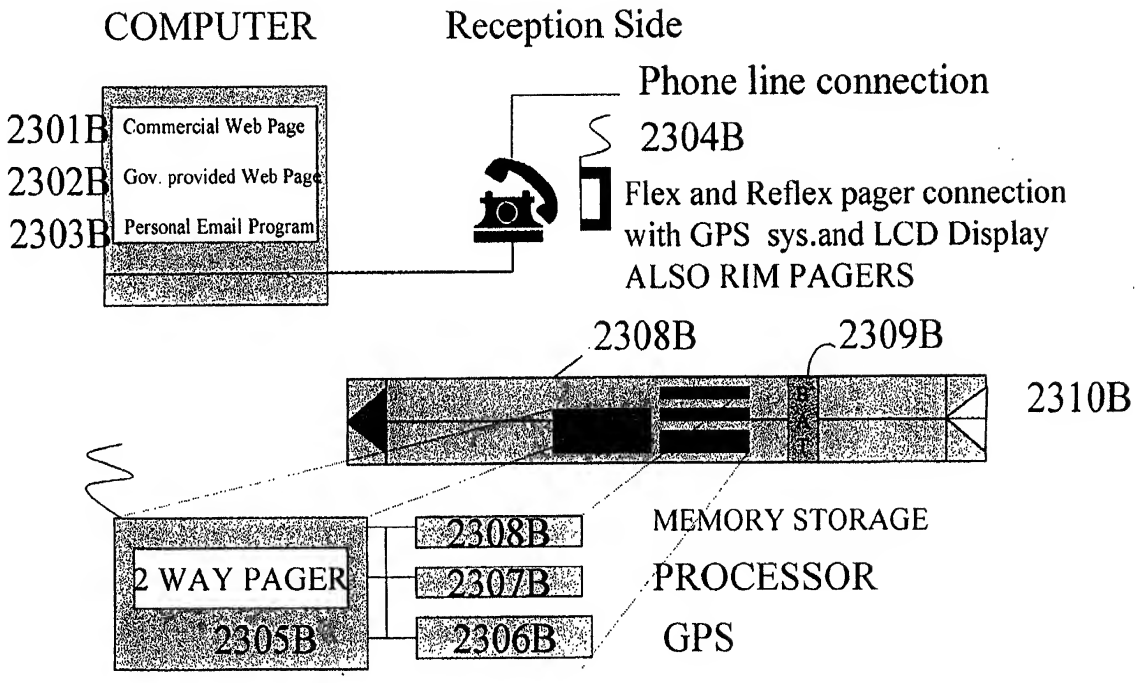


FIG.23b PAGER TRACKING FOR PERSONAL PFN'S



09/018095

14/14

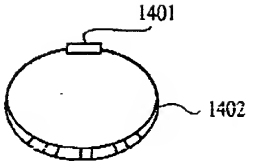


FIG. 13A

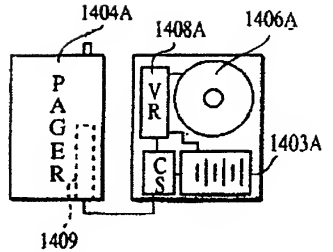


FIG. 13C

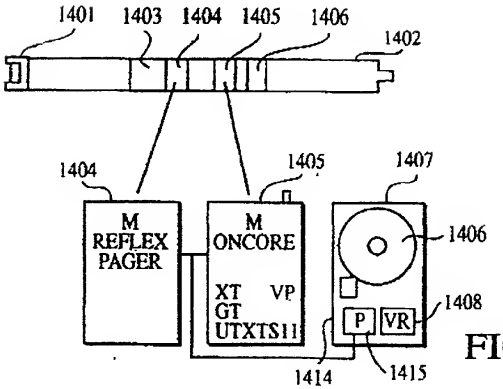


FIG. 13B

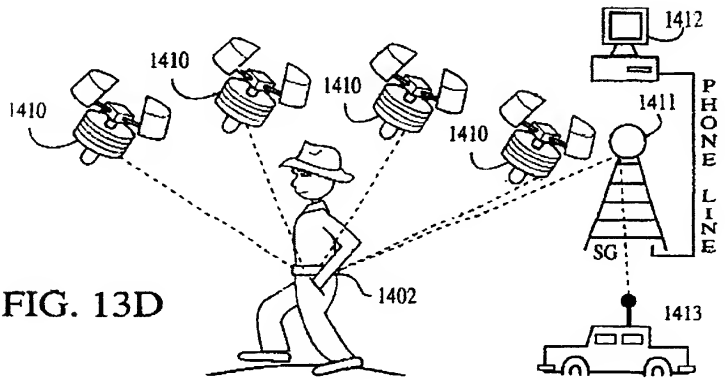


FIG. 13D

FIG. 23C

CELLLULAR PHONE TRACKING FOR PERSONAL PFN

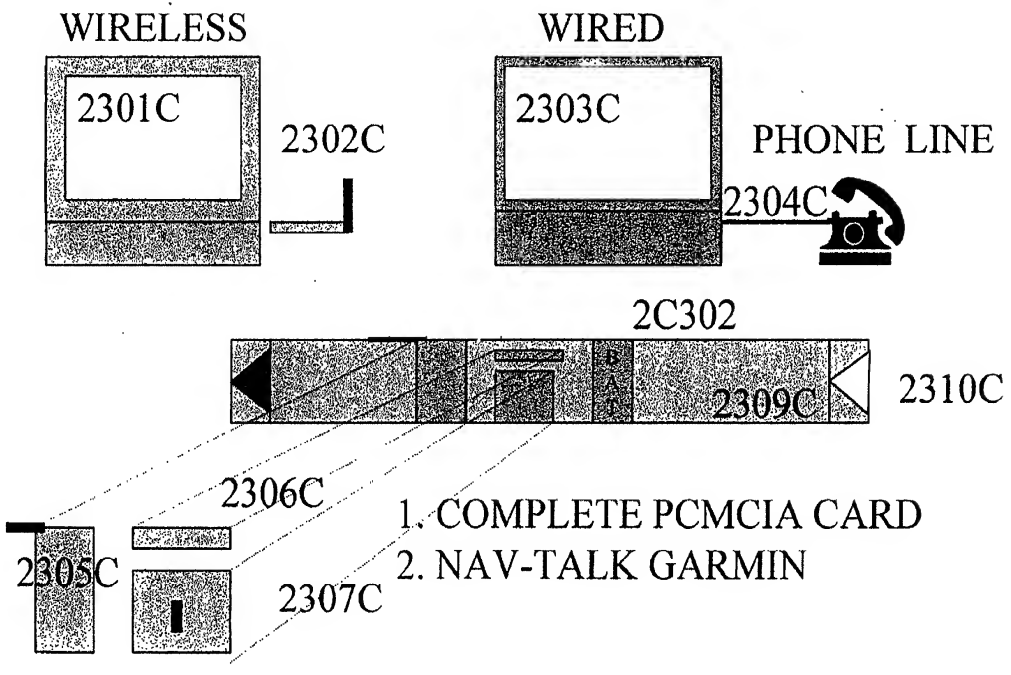


FIG 23D

NEXTEL, RADIO, PAGER, AND PHONE

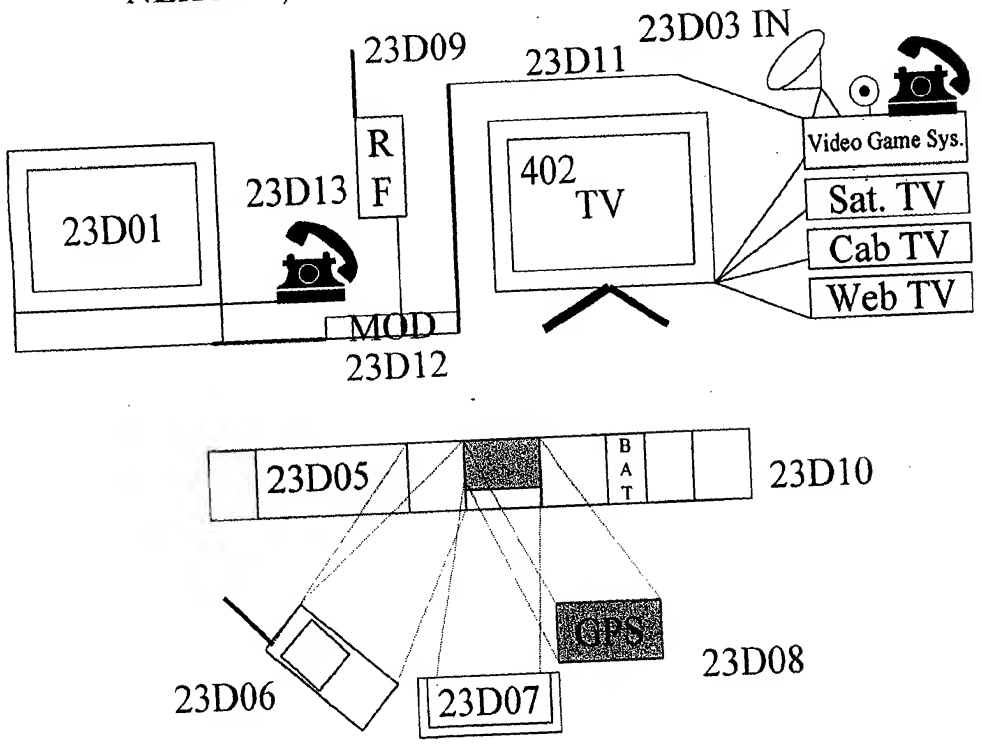


FIG. 23E

BELT, CLASP, COLLAR OR BRACELET SECURITY SYSTEM

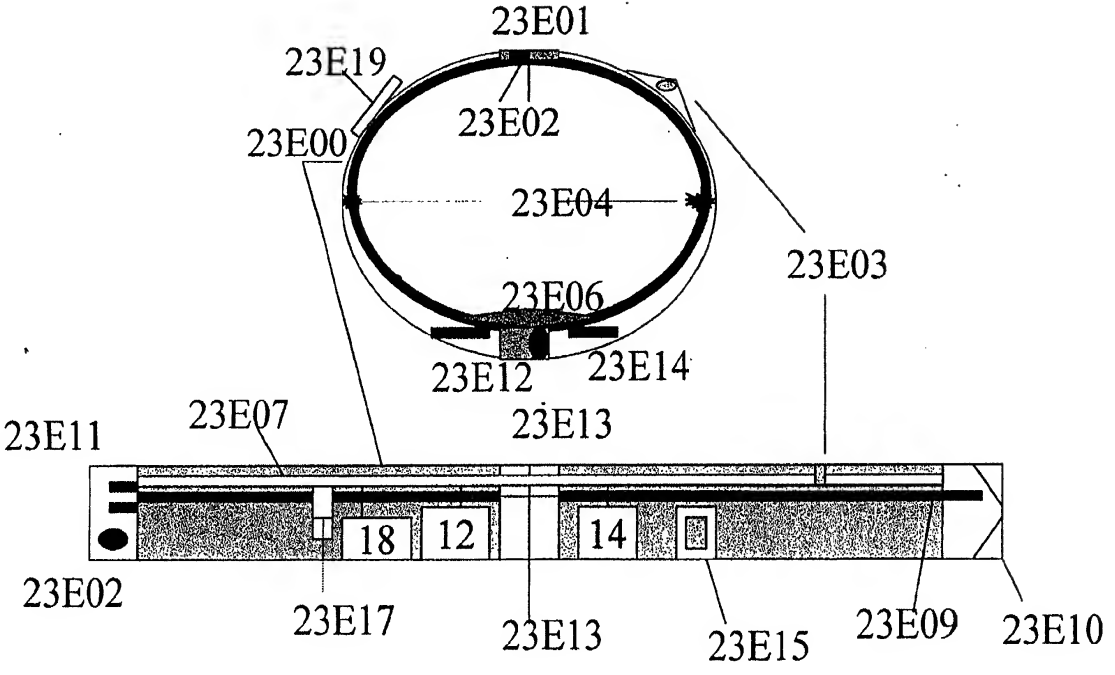


FIG. 24 PERSONAL PRODUCTS & APPLICATIONS

RF REPEATER SYSTEMS
TOT SPOT,
HUNT WELL
PET POINTER,
FRIEND FINDER

WIRELESS PAGER AND TELEPHONY
TRAC A CON . COM/GOV
SKI SEARCHER
SWIM SEAKER
FAMILY FINDER
PATIENT PAL OR HEALTH WATCH
LOST AND FINDER
PEOPLE LOCATOR
PET LOCATOR
PHYSICAL TELEMETRY
IDENTITY CONFIRM ATION

*ALL PRODUCT NAMES STATED HERE ARE PROPRIETARY TO KLINE AND WALKER LLC AND COMMERCIAL USE IS GOVERNED BY LICENSING AUTHORITY

ACTIVITY CONTROLS
AUDIO & VIDEO
P.I.N.- SYSTEMS(IDENTITY)
HEALTH CARE
AUTOMATED MEDICATIONS
BEHAVIOR SUPRESSION SYS.
SEDITIVES
SHOCKING
DECRETES IN ALL CONTROLS

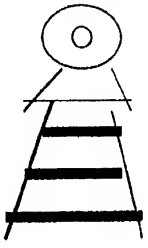
SENSORY TELEMETRY
BLOOD PRESSURE
HEART RATE
CHEMICAL SENSORS
WATER
HEAT
DRUG SENSORS
DESCRETES, EMF,RADIATION
APPLICATION SPECIFIC

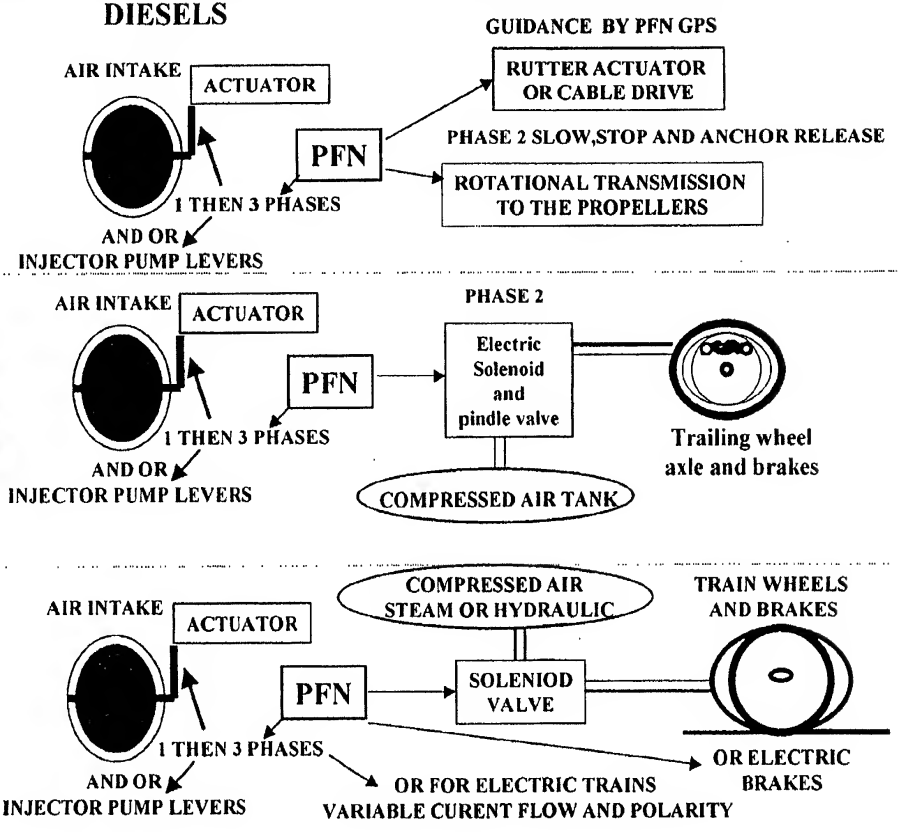
ACCOUNABILITY
MEMORY STORAGE
REMOTE MEMORY
LOCAL MEMORY

FIG 25

MANAGEMENT PFNS FOR OTHER VEHICLES AND MACHINERY

DIESELS





WO 00/78057
64/64
PCT/US00/16381

Docket No.: 110273-500 US1 **PATENT/OFFICIAL**

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter claimed and for which a patent is sought on the invention entitled **SECURE, ACCOUNTABLE, MODULAR AND PROGRAMMABLE SOFTWARE TRAC**, the specification of which was filed on 14 December 2001 as Application Serial No. 10/018,095 .

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is known to me to be material to patentability in accordance with Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d) or Section 365(b) of any foreign application(s) for patent or inventor's certificate, or Section 365(a) of any PCT international application which designated at least one country other than the United States, listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s):			**Priority Claimed**	
Number	**Country**	**Day/Month/Year filed**	**Yes**	**No**

I hereby claim the benefit under 35 USC '119(e) of any United States provisional application(s) listed below.

Prior Provisional Application(s):

Application Number	**Filing Date**
60/139,759	**15 June 1999**
60/176,818	**19 JAN 2000**
60/200,872	**1 MAY 2000**

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s), or Section 365(c) of any PCT international application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, Section 1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Prior U. S. Application(s):

Serial No.	**Filing Date**	**Status: Patented, Pending, Abandoned**
PCT/US001/16381	15 June 2000	pending

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

The undersigned hereby grant(s) the firm of HALE AND DORR LLP the power to insert on this Declaration any further identification, including the application number and filing date, which may be necessary or desirable in order to comply with the rules of the United States Patent and Trademark Office for recordation of this document

The undersigned Principal Attorney of record hereby appoints the registered practitioner(s) listed at the following customer number, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith, and, in addition please direct all correspondence to the address at the following customer number:

24395

HALE AND DORR
1455 Pennsylvania Avenue, NW
Washington, DC 20004
TEL 202.942.8400
FAX 202.942.8484

****

Full name of sole or first inventor: Richard C. Walker

Inventor's signature: Richard C. Walker Date: 4/18/02

Residence: Waldorf, Maryland USA MD

Citizenship: USA

Post Office Address: 11201 Spur Wheel Lane, Potomac, MD 20854 USA

****

Full name of second joint inventor:

Inventor's signature: Date:

Residence:

Citizenship:

Post Office Address:

****

Full name of second joint inventor:

Inventor's signature: Date:

Residence:

Citizenship:

Post Office Address:

168090v1